ISABELA DRAGO

SEGURANÇA DA INFORMAÇÃO: ESTUDO EXPLORATÓRIO EM ORGANIZAÇÕES DE GRANDE PORTE DO MUNICÍPIO DE CURITIBA

Monografia apresentada à Disciplina de Projeto de Pesquisa em Informação II do Curso de Gestão da Informação, do Setor de Ciências Sociais Aplicadas, da Universidade Federal do Paraná.

Orientadora: Prof. Patricia Zeni Marchiori

CURITIBA

2004

SUMÁRIO

LISTA DE TABELAS

LISTA DE QUADROS E ILUSTRAÇÕES

LISTA DE ANEXOS

RESUMO

Identifica na literatura pertinente e na NBR ISO/IEC 17799 conceitos e princípios da segurança da informação, comparando a veracidade de tais conceitos e princípios com uma pesquisa de campo em empresas de grande porte situadas no município de Curitiba. Do universo da pesquisa, composto de vinte duas empresas, extraiu-se uma amostra de 19 empresas das quais foram analisadas dez, confirmando que as empresas estão cientes da importância da temática, e mesmo não aplicando a NBR ISO/IEC 17799, as mesmas possuem procedimentos relacionados à segurança das suas informações. Outro fator verificado é que apesar da segurança da informação envolver tanto aspectos tecnológicos (escola técnica) quanto aspectos relacionados à cultura organizacional (escola não técnica), ainda assim, as empresas estão focadas nas questões tecnológicas, abordando apenas de maneira superficial as questões não técnicas.

Palavras-chave: Segurança da informação; NBR ISO/IEC 17799; aspectos técnicos; e cultura organizacional.

1 INTRODUÇÃO

"Na sociedade em que vivemos, onde a informação é grande fonte de riqueza (e, portanto, um dos principais ativos a serem protegidos), subestimar a importância da segurança pode custar a sobrevivência da organização no mercado". (NIMER, 1998, p.24).

Segurança da informação é o elemento chave dentro da organização: envolve aspectos técnicos, humanos e organizacionais, sendo fundamental a definição e existência de uma política para efetiva proteção das informações Portanto, segurança da informação não deve ser vista simplesmente como um "guardar num cofre todas as informações disponíveis", mas para realmente alcançá-la, torna-se necessário elaborar políticas de proteção das informações a fim de se evitarem maiores riscos e vulnerabilidades.

A segurança da informação tem deixado de ser tratada meramente como um assunto técnico da área de informática, e vem sendo considerada uma real necessidade nas empresas e nas instituições, visto que a informação é o bem ativo mais valioso de uma empresa. A segurança passa a ser um requisito estratégico, que interfere na capacidade das organizações de realizarem negócios e no valor de seus produtos no mercado.

Uma política de segurança da informação deve ser composta por regras claras, praticáveis e sintonizadas com a cultura e o ambiente tecnológico da empresa. Deve não apenas proteger as informações confidenciais, mas também motivar as pessoas que as manuseiam, mediante a conscientização e envolvimento de todos. Garantir a segurança organizacional é um grande desafio, que passa por todas as pessoas direta e indiretamente envolvidas.

Segurança é, portanto, a proteção de informações, sistemas, recursos e serviços contra desastres, erros e manipulação não-autorizada, de forma a reduzir a probabilidade e o impacto de incidentes de segurança.

Em face do exposto acima, pretende-se neste estudo identificar as condições de Segurança da Informação nas empresas de grande porte do município de Curitiba, considerando tanto as dimensões tecnológicas como as dimensões relativas a cultura organizacional, tendo como base a literatura pertinente e a NBR ISO/IEC 17799.

Pretende-se também, por meio de uma pesquisa de campo, verificar as condições existentes, em empresas de grande porte do município de Curitiba, que

podem refletir uma preocupação relativa a procedimentos de segurança de informação e identificar o potencial uso da NBR ISO/IEC 17799.

2 O PROBLEMA E A JUSTIFICATIVA

Na era do conhecimento, onde a informação é considerada um dos principais patrimônios de parte expressiva das organizações, ela deve ser tratada como tal, devendo ser protegida nos seus aspectos de disponibilidade, integridade e confidencialidade. Isto porque segurança de informações é um elemento chave dentro desses conceitos, podendo ser considerada parte do ambiente informacional. O ambiente informacional, detalhando por DAVENPORT (1998), engloba princípios básicos de política da informação, cultura e comportamento em relação à informação, equipe da informação, processos de administração informacional e arquitetura da informação e, ainda que autor não se refira especificamente ao conceito de **Segurança da Informação**, é possível especular que o ambiente informacional pode englobar mais essa faceta até mesmo como um elemento transversal aos demais elementos, influenciando-os e sendo influenciado por eles.

A partir da década de 70, o interesse mundial pela segurança da informação cresceu e, depois de 30 anos, pode-se falar da existência de duas escolas dentro da temática relativa à segurança da informação: a **escola técnica** que concentra-se somente nos aspectos tecnológicos e a **escola não-técnica** que engloba aspectos relacionados à cultura organizacional, conforme comentado por BASKERVILLE e SIPONEN (2002, p. 337).

O conjunto de estudos de caso e esforços contínuos, relacionados com a busca de melhores mecanismos para resguardar a segurança da informação, resultou, em 2001, na homologação da Norma Internacional de Segurança da Informação denominada NBR ISO/IEC[1] 17799. A Norma é definida como um código de prática para a gestão da segurança da informação, abordando tanto as dimensões tecnológicas como as dimensões relativas a cultura organizacional.

---

[1] **IEC** - (*International Electrotechnical Commission*): organização que, conjuntamente com a ISO, desenvolve, sugere e define padrões para protocolos de rede.

ISO - (*International Organization for Standardization*): organização internacional que desenvolve, sugere e define padrões.

NBR - Norma Brasileira.

Contudo, o tema tem exploração recente no Brasil, pois o mesmo só começou a ser discutido nos anos 90 devido ao aumento das vulnerabilidades dos sistemas acarretado, em grande parte, pela expansão do uso e acesso à Internet nos ambientes organizacionais.

Paul Breslin, gerente de projetos da *Det Norke Veritas* (DNV), em entrevista no artigo "Certificação 17799: uma visão internacional" (2003), aponta quais benefícios as empresas brasileiras obteriam com a adoção da Norma:

> Primeiro, são os benefícios internos, através da melhoria do gerenciamento de sua própria informação, garantindo assim para os sócios e parceiros da empresa uma avaliação competente e imparcial sobre o seu sistema de segurança da informação. Outra vantagem é possibilitar conformidade com à legislação nacional de segurança da informação de seu país, como por exemplo, ajudar as organizações a cumprirem as exigências de leis sobre privacidade de dados.

No recente artigo "Perspectivas 2003 para o mercado de segurança da informação", o gerente Nacional de produtos da Empresa *Módulo Security*[2], Marcos Sêmola, referindo-se a norma, afirma que "o crescimento exponencial do interesse pela conformidade, seja com objetivos de marketing, fortalecimento da imagem ou criticidade do negócio e sua operação, tornam promissor este padrão" (2003). Apesar dessa afirmação o autor identificou, naquele momento, apenas duas empresas no Brasil que estavam aplicando efetivamente a Norma.

Ainda que o tema esteja sendo cada vez mais discutido e a NBR ISO/IEC 17799 esteja sendo reconhecida como um "padrão promissor", considera-se que a maioria das empresas brasileiras ainda se mostra relutante em adotar medidas de segurança ou sistemas de prevenção contra ataques internos e externos, devido, em especial aos altos custos envolvidos. Outro motivo para essa relutância, é que muitos executivos precisam de números precisos para tomar decisões financeiras, mas que, em termos de segurança isso nem sempre é possível, já que sempre trabalha-se com a "probabilidade" da ocorrência de um incidente. Assim, o retorno sobre investimento em segurança não deveria ser somente analisado em termos quantitativos, como normalmente ocorre (CRISTONI, 2000, p. 8-9).

Considerando que a Segurança da Informação pode ser identificada como mais um princípio geral dentro das empresas, torna-se relevante investigar as condições em que a própria Norma é utilizada ou mesmo de maneira geral como as

---

[2] **EMPRESA MÓDULO SECURITY.** Disponível em: <http://www.modulo.com.br> Acesso em: 14 maio 2004.

empresas percebem a importância da aplicação de requisitos relacionados a segurança da informação de maneira mais ampla.

Considerando-se ainda, que nenhum trabalho acadêmico tenha sido realizado sobre este tema, até o momento, no Curso de Gestão da Informação da Universidade Federal do Paraná, este trabalho propõe a verificação das condições de utilização de procedimentos de Segurança de Informação em empresas de grande porte do Município de Curitiba, com base nas orientações da NBR ISO/IEC 17799 e na literatura pertinente da área.

Diante das diferentes facetas relacionadas ao tema proposto pode-se levantar as seguintes questões de pesquisa:

a) Empresas de grande porte do município de Curitiba aplicam a NBR ISO/IEC 17799? Caso não apliquem a norma, estabelecem procedimentos relacionados ao que se considera, de forma ampla, “segurança da informação”?

b) os custos de implantação podem ser um empecilho para a aplicação de mecanismos de segurança da informação nas empresas de grande porte do município de Curitiba?

c) independentemente da aplicação da Norma, aquelas empresas de grande porte do município de Curitiba que se preocupam em definir procedimentos relacionados a “segurança da informação”, o fazem voltados mais à tecnologia da informação (escola técnica) do que à cultura organizacional (escola não técnica)?

Com o desenvolvimento desta pesquisa pretende-se verificar os conceitos de segurança da informação e sob que aspectos a temática é tratada e discutida no universo selecionado.

Empiricamente, pode-se dizer que há um predomínio da área de Informática nos processos relativos à segurança da informação. Todavia, o presente estudo pode levantar aspectos relacionados a gestão da informação conforme o perfil de formação da Universidade Federal do Paraná, demonstrado assim que, para o

Gestor da Informação, existem perspectivas ainda não exploradas no mercado de trabalho.

Provavelmente esta intervenção, tendo em vista seu caráter exploratório, irá fazer com que a pesquisadora entre em contato com as empresas, o que estimulará reflexão nas mesmas sobre o tema “segurança da informação”.

Outrossim, o presente trabalho estará disponível como referência para a área, uma vez que, igualmente, se pretende dar sugestões de continuidade sobre o assunto.

3 OBJETIVOS

3.1 OBJETIVO GERAL

Identificar as condições de Segurança da Informação nas empresas de grande porte do município de Curitiba, com visão nas dimensões tecnológicas e nas dimensões relativas a cultura organizacional, tendo como base literatura pertinente e a NBR ISO/IEC 17799.

3.2 OBJETIVOS ESPECÍFICOS

- Caracterizar a Segurança da Informação em ambientes informacionais de empresas de grande porte do município de Curitiba;

- Conceituar princípios relacionados a Segurança da Informação considerando aspectos tecnológicos e cultura organizacional, em especial com base na NBR ISO/IEC 17799;

- Verificar as condições existentes, em empresas de grande porte do município de Curitiba, que podem refletir uma preocupação relativa a procedimentos de segurança de informação e o potencial uso da NBR ISO/IEC 17799.

4 REFERENCIAL TEÓRICO

4.1 RECURSO ESTRATÉGICO: INFORMAÇÃO

A Informação assume, hoje em dia, uma importância crescente. Ela se torna fundamental na empresa, tanto na descoberta e introdução de novas tecnologias, como na exploração das oportunidades de investimento e, ainda, na planificação de toda a atividade industrial.

Na realidade, existem muitas e variadas definições de informação, que diferem em complexidade. Segundo ZORRINHO (1995, p. 32) informação “é um processo que visa o conhecimento, ou, mais simplesmente, informação é tudo o que reduz a incerteza. (...) Um instrumento de compreensão do mundo e da ação sobre ele". Para FERREIRA (1995, p. 170) “informação é um dado acerca de alguém ou algo; o conhecimento; segundo a teoria da informação, a medida da redução da incerteza”.

Abstraindo-se desta complexidade, pode-se afirmar que a informação tornou-se uma necessidade crescente e indispensável para qualquer setor da atividade humana, mesmo que a sua procura não seja ordenada ou sistemática, mas resultante apenas de decisões casuais e/ou intuitivas.

Uma empresa em atividade é, por natureza, um sistema aberto e interativo suportado por uma rede de processos articulados, onde os canais de comunicação existentes dentro da empresa e entre esta e o seu meio envolvente são irrigados por informação (ZORRINHO, 1995, p. 32).

Atualmente, as empresas estão envolvidas num meio bastante turbulento com características diferentes das habituais e os gestores percebem que, em alguns casos, a mudança é a única constante. DRUCKER (1993, p. 22) ilustra isso afirmando que "desde que me lembro, o mundo dos gestores tem sido turbulento,...certamente até muito turbulento, mas nunca como nos últimos anos, ou como será nos mais próximos."

Por conseguinte, vários acontecimentos externos obrigam as organizações a enfrentar novas situações, resultado de mudanças no mercado e que constituem ameaças e/ou oportunidades para as empresas, fazendo com que tomar decisões hoje, exija a qualquer empresário ou gestor estar bem informado e conhecer o

mundo que o rodeia. O aumento da concorrência e da complexidade do meio ambiente fazem sentir, no mundo empresarial, a necessidade de se obterem melhores recursos do que os dos seus concorrentes e de otimizar a sua utilização.

O aumento do comércio internacional, fruto da crescente interligação entre nações, a expansão do investimento no exterior e a tendência da homogeneização dos padrões de consumo fazem com que o mundo seja encarado como um só mercado, em que as empresas têm de conviver com a competição internacional, e ao mesmo tempo, tentarem penetrar nos mercados externos por forma a aproveitar as novas oportunidades de negócio.

Assim, a empresa ao atuar num mundo global está em estado de "necessidade de informação" permanente, em vários níveis, reconhecendo-se que a informação constitui o suporte de uma organização e é um elemento essencial e indispensável a sua existência. A aceitação deste papel, pelos dirigentes de uma organização pode ser um fator imprescindível para se atingir uma situação de excelência: quem dispõe de informação de boa qualidade, fidedigna, em quantidade adequada e no momento certo, adquire vantagens competitivas mas a falta ou perda de informação dá margem a erros e a perda de oportunidades.

A informação tornou-se tão importante que DRUCKER (1993, p. 25) defende “o primado da informação como a base e a razão para um novo tipo de gestão, em que a curto prazo se perspectiva a troca do binômio capital/trabalho pelo binômio informação/conhecimento como fatores determinantes no sucesso empresarial. Caminha-se para a sociedade do saber onde o valor da informação tende a suplantar a importância do capital”. O autor ainda enfatiza que “a informação e o conhecimento são a chave da produtividade e da competitividade”.

A gestão moderna exige que a tomada de decisão seja feita com o máximo de informação. O conhecimento adquirido pelo “saber fazer” deixa de ser suficiente, uma vez que o meio ambiente empresarial onde as empresas operam apresenta características diferentes daquelas a que estavam habituados e é bastante dinâmico.

Portanto, se em ambientes mais estáveis a informação assumia o papel de redutora de incerteza, cada vez mais a atualização se apresenta como um fator crítico de sucesso. Verificando toda essa mudança pode-se afirmar que todas as empresas deverão fazer uma reestruturação organizacional em torno da informação.

É aqui que deve ter lugar a gestão da informação, a gestão de tecnologias de informação e, mais especificadamente, a **segurança da informação**, como um dos componentes de vantagem competitiva.

4.2 CONCEITOS DE SEGURANÇA DA INFORMAÇÃO

Segundo alguns conceitos básicos de autores para fundamentação deste trabalho, pode-se considerar a segurança da informação, de forma geral, como um conjunto de dados, imagens, textos e outras formas de representação usadas para os valores da Companhia, associados ao seu funcionamento e/ou manutenção das suas vantagens competitivas.

Segurança da Informação conforme definido pela NBR ISO/IEC 17799 (2001, p. 2) “é a proteção contra um grande número de ameaças às informações, de forma a assegurar a continuidade do negócio, minimizando danos comerciais e maximizando o retorno de investimentos e oportunidades”. A segurança da informação é caracterizada pela preservação dos seguintes atributos básicos (NBR ISO/IEC 17799, 2001, p. 4):

a) Confidencialidade: garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso;
b) Integridade: salvaguarda da exatidão e precisão da informação e dos métodos de processamento;
c) Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Conforme FIGUEIRÊDO (2002, p. 4), os componentes de uma política de segurança da informação podem ser definidos como:

a) Recursos de Informação - são todos os meios usados para obtenção, geração, armazenamento e transporte das informações. Inclui: os recursos do ambiente de tecnologia da informação (instalações e equipamentos de informática e telecomunicações, sistemas operacionais, aplicativos e sistemas de informação usados nesses equipamentos) e

outros recursos convencionais (arquivos, papel, microfilme, mapas, entre outros).

b) Sistema de Informação - é um conjunto de processos e recursos do ambiente de tecnologia da informação organizados para prover, de modo sistemático, informações para a Companhia.
c) Órgão Proprietário da Informação - é o órgão da empresa responsável pelas informações de uma determinada área de atividade da Companhia.
d) Proprietário da Informação - empregado, designado pelo Órgão Proprietário da Informação, para responder perante a Companhia pela classificação das informações e definição das suas necessidades de segurança.
e) Comitê de Segurança de Informações - é o comitê constituído pela Diretoria Executiva da empresa com a finalidade de implantar e garantir o cumprimento da Política de Segurança de Informações no âmbito da Companhia.
f) Gerente de Segurança de Informações do Órgão - empregado designado pelo órgão da Companhia, como responsável pelo cumprimento da Política de Segurança de Informações no âmbito do órgão, servindo de interface entre gerentes, proprietários, usuários, custodiantes, Gerência de Tecnologia da Informação do Órgão e o Comitê de Segurança de Informações.

Importante destacar que a NBR ISO/IEC 17799 (2001, p. 2) informa que a "Segurança da Informação é obtida a partir da implementação de uma série de controles, que podem ser políticas, práticas, procedimentos, estruturas organizacionais e funções de *software*". Estes controles precisam ser estabelecidos para garantir que os objetivos da segurança da informação sejam atendidos.

Um número de controles pode ser considerado como princípios básicos, fornecendo um ponto de partida consistente para a implementação da segurança da informação. Conforme consta na NBR ISO/IEC 17799, esses princípios são baseados tanto em requisitos legais como nas melhores práticas de segurança da informação.

Os controles considerados essenciais para uma organização, sob o ponto de vista legal, incluem (NBR ISO/IEC 17799, p. 3):

a) Proteção de dados e privacidade de informações pessoais;
b) salvaguarda de registros organizacionais;
c) direitos de propriedade intelectual.

Já os controles considerados como melhores práticas para a segurança da informação incluem (NBR ISO/IEC 17799, p. 3):

a) Documento da política de segurança da informação;
b) definição das responsabilidades na segurança da informação;
c) educação e treinamento em segurança da informação;
d) relatório dos incidentes de segurança;
e) gestão da continuidade do negócio.

Após a verificação de alguns conceitos e princípios básicos, a exploração do tema segue, apontando alguns objetivos da segurança da informação dentro do contexto técnico e não técnico que envolve o tema.

4.3 OBJETIVOS DA SEGURANÇA DA INFORMAÇÃO

Quando se pensa em segurança da informação, a primeira idéia que vem à mente é a proteção da mesma, não importando onde ela esteja. Um sistema computacional é considerado seguro se houver uma garantia de que é capaz de atuar exatamente como esperado. Porém, segurança é um conceito que vai muito além disso. É expectativa de todos que a informação armazenada em um sistema computacional permaneça lá, sem que pessoas não autorizadas tenham acesso a seu conteúdo. Ou seja, é a expectativa de qualquer usuário que as informações estejam em local adequado, disponíveis no momento desejado, que sejam confiáveis, corretas e permaneçam protegidas contra acessos indesejados. Essas expectativas correspondem aos objetivos gerais da segurança da informação.

Destacam-se entre, os aspectos tecnológicos, os objetivos da segurança da informação (FIGUEIRÊDO, 2002, p. 4):

a) Confidencialidade ou privacidade – proteger as informações contra acesso de qualquer pessoa não autorizada pelo gestor da informação[3]. Este objetivo envolve medidas como controle de acesso e criptografia.
b) Integridade dos dados – evitar que dados sejam apagados, ou alterados sem a permissão do gestor da informação.
c) Legalidade - Estado legal da informação, em conformidade com os preceitos da legislação em vigor.
d) Disponibilidade – garantir o provimento do serviço de informática, sob demanda, sempre que necessário aos usuários autorizados. As medidas relacionadas a esse objetivo podem ser duplicação de equipamentos/sistemas e *backup*. Um bom exemplo de ataque contra disponibilidade é a sobrecarga provocada por usuários ao enviar enormes quantidades de solicitação de conexão com o intuito de provocar pane nos sistemas.
e) Consistência – certificar-se de que o sistema atua de acordo com a expectativa dos usuários.
f) Isolamento ou uso legítimo – controlar o acesso ao sistema. Garantir que somente usuários autorizados possuam acesso ao sistema.
g) Auditoria – proteger os sistemas contra erros e atos cometidos por usuários autorizados. Para identificar autores e ações, são utilizadas trilhas de auditorias e *logs*, que registram o que foi executado no sistema, por quem e quando.
h) Confiabilidade – garantir que, mesmo em condições adversas, o sistema atuará conforme esperado.

Segundo a NBR ISO/IEC 17799 (2001, p. 2) “a segurança da informação que pode ser alcançada por meios técnicos é limitada e convém que seja apoiada

[3] Segundo FONTES (2004) compreende-se por gestor da informação “a pessoa responsável pela liberação (ou não) da informação para toda a empresa e também deve ser responsável pela continuidade do negócio no que depende daquela informação. Um Gestor consciente da sua função será um aliado para a obtenção e manutenção de recursos para a proteção da informação. E esse Gestor deve estar definido na Política de Segurança da Informação”.

por gestão e procedimentos apropriados. A gestão da segurança da informação necessita, pelo menos, da participação de todos os funcionários da organização".

Portanto, antes de implementar um programa de segurança da informação, é imprescindível levar em consideração tanto os aspectos tecnológicos quanto os aspectos relacionados a cultura organizacional. DIAS (2000, p. 4) destaca que para implementar um programa de segurança da informação é aconselhável responder às seguintes questões:

a) o que proteger?

b) contra que ou quem?

c) quais as ameaças mais prováveis?

d) qual a importância de cada recurso?

e) qual o grau de proteção desejado?

f) quanto tempo, recursos humanos e financeiros se pretende gastar para atingir os objetivos de segurança desejados?

g) quais as expectativas dos usuários e clientes em relação à segurança de informações?

h) quais as conseqüências para a instituição se seus sistemas e informações forem violados ou roubados?

Tendo a resposta a essas perguntas, é definida a política de segurança das informações e analisadas as ameaças, fazendo-se uma **análise de riscos**. A tecnologia de segurança a ser implantada deve, portanto, atender aos requisitos da política.

Por fim, para administrar os sistemas, é necessário implantar uma gerência de segurança que preocupe-se tanto com o aspectos propriamente tecnológicos quanto com os aspectos culturais da organização.

Segurança da informação é a conjugação de uma estratégia e de ferramentas específicas que atendam as necessidades corporativas para a manutenção de um ambiente saudável. Considerada um item vivo, a política de segurança nunca está acabada e deve ser desenvolvida e atualizada durante toda a vida da empresa (COLTRO, 2002, p. 26).

Conforme será explicitado a seguir, a análise de riscos pode ser considerada peça fundamental para a obtenção da qualidade de uma política da segurança da informação, pois a mesma ajudará a identificar todos os pontos críticos e falhos de

proteção em todos os processos, configurações, documentos. Isto é, tudo que possa ser valioso para a atividade da organização. A análise de riscos fornecerá também, diretrizes para a identificação das medidas de segurança necessárias para que o ambiente informacional da organização possa atingir o nível de segurança desejado.

4.4 A ANÁLISE DE RISCOS COMO PRESSUPOSTO PARA A SEGURANÇA DA INFORMAÇÃO

Muitas vezes o termo risco é utilizado como sinônimo de ameaça ou da probabilidade de uma ameaça ocorrer. Para DIAS (2000, p. 54) “risco é uma combinação de componentes, tais como ameaças, vulnerabilidades e impactos. A análise de riscos engloba tanto a análise de ameaças e vulnerabilidades quanto a análise de impactos, a qual identifica os componentes críticos e o custo potencial ao usuário do sistema”. DIAS (2000, p. 54) ainda destaca que a “análise de riscos é o ponto chave da política de segurança da informação”.

Conforme consta em MOREIRA (2001, p. 11):

> a análise de risco consiste em um processo de identificação e avaliação antecipada dos fatores de risco presentes no Ambiente Organizacional, possibilitando uma visão do impacto negativo causado aos negócios. Através da aplicação desse processo, é possível determinar as prioridades de ação em função do risco identificado, para que seja atingido o nível de segurança desejado pela Organização. Proporciona também informações para que se possa identificar, antecipadamente, o tamanho e o tipo de investimento necessário para prevenir os impactos na Organização causados pela perda ou indisponibilidade dos recursos fundamentais para o negócio.

Vale ressaltar que os riscos podem ser apenas reduzidos, já que é impossível eliminar todos os riscos. Tomando medidas de segurança mais rígidas, os riscos podem ser cada vez menores, mas nunca serão totalmente eliminados.

Contudo, com o processo da análise de riscos é possível adquirir as informações importantes, tais como (MOREIRA, 2001, p.12):

a) pontos vulneráveis do ambiente;
b) ameaças potenciais ao ambiente;
c) incidentes de segurança causado pela ação de cada ameaça;
d) impacto negativo para o negócio a partir de cada incidente de segurança;
e) medidas de proteção adequadas para impedir ou diminuir o impacto de cada incidente.

Conhecer com antecedência as ameaças informacionais e seus impactos pode resultar em medidas efetivas para reduzir as ameaças, as vulnerabilidades e, consequentemente, os impactos. Agindo de maneira proativa, pode-se facilitar e tornar menos onerosas as medidas corretivas.

Portanto, conforme explicitou DIAS (2000, p. 54), “o objetivo da análise de riscos é medir ameaças, vulnerabilidades e impactos em um determinado ambiente, de forma a proporcionar a adoção de medidas apropriadas tanto às necessidades de negócio da instituição, ao proteger seus recursos de informação, como aos usuários, que precisam utilizar esses recursos, levando em consideração justificativas de custos, nível de proteção e facilidade de uso”.

4.4.1 Análise de Ameaças e Vulnerabilidades

Antes de decidir como proteger um sistema, por exemplo, é necessário saber contra o que ele será protegido. A segurança pode, então, ser definida em termos de combate às ameaças identificadas.

Segundo DIAS (2000, p. 56) “ameaça é tudo aquilo que pode comprometer a segurança de um sistema, podendo ser acidental (falha de *hardware*, erros de programação, desastres naturais, erros do usuário, *bugs* de *software*, uma mensagem secreta enviada a um endereço incorreto, etc.) ou deliberada (roubo, espionagem, fraude, sabotagem, invasão de *hackers*, entre outros)”. Ameaça pode ser uma pessoa, uma coisa, um evento ou uma idéia capaz de causar dano a uma recurso, em termos de confidencialidade, integridade e disponibilidade.

As ameaças exploram as vulnerabilidades do ambiente informacional para causar impactos. A análise dessas ameaças e vulnerabilidades tenta definir a probabilidade de ocorrência de cada evento adverso e as conseqüências da quebra de segurança.

MOREIRA expõe (2001, p. 27) que existem vulnerabilidades presentes em muitos ambientes, e que muitas organizações não atentam para determinadas situações, tais como:

a) senhas fracas;
b) falhas de implementação da segurança da informação;
c) deficiência na política de segurança da informação;

d) manuseio inadequado de informações confidenciais/críticas.

BASTOS (2004) afirma que “as principais vulnerabilidades encontradas costumam ser relativas a erros, acidentes ou desconhecimento dos usuários que, impensadamente alteram configurações de equipamentos, divulgam contas e senhas de acesso, deixam sessões abertas na sua ausência, utilizam senhas frágeis facilmente descobertas (como o próprio nome ou palavras comuns) ou mesmo contaminam seus arquivos e programas com vírus de computadores.”

4.4.2 Análise de Impactos

DIAS (2000, p. 57) explica que “a análise de impactos identifica os recursos críticos do sistema, isto é, recursos que mais sofrerão impactos na ocorrência de uma quebra de segurança”. Portanto, o objetivo da análise de impactos é identificar funções, sistemas e recursos e classificá-los de acordo com sua importância para a organização.

Normalmente os impactos são analisados sob dois aspectos: curto prazo e longo prazo, em função do tempo em que o impacto, causado por uma ameaça, permanece afetando os negócios da organização.

Durante a análise de impactos é recomendável que sejam entrevistados gerentes de diversas áreas de negócio, pois há vários tipos de impactos intrinsecamente relacionados aos negócios da organização que, por isso, devem ser definidos pelas pessoas que mais os conhecem. Além disso, torna-se possível avaliar a importância de cada atividade, sistema e recurso e ainda identificar suas vulnerabilidades e possíveis ameaças.

Em termos administrativos, geralmente os impactos são classificados como (DIAS, 2000, p. 114):

a) Diretos: são aqueles que envolvem perdas financeiras (reposição ou reparação de equipamentos, por exemplo), diminuição da receita, aumento de custos ou penalidades financeiras pelo descumprimento de contratos, por exemplo.
b) Indiretos: são aqueles que não envolvem diretamente perdas financeiras, mas podem originá-las. Nessa categoria se encontram o descumprimento

da lei, a perda da reputação e credibilidade no mercado, os conflitos com acionistas, políticos, sindicatos, etc.

Conforme verificou-se, a combinação desses dois tipos de análises (análise de ameaças e vulnerabilidades e análise de impactos) compõem a chamada análise de riscos, que é utilizada para justificar as medidas de segurança da informação a serem implantadas pela organização, através de uma política de segurança da informação.

4.5 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Pode-se, de maneira geral, caracterizar a política da segurança da informação como um conjunto de normas que definem as melhores práticas para o manuseio, armazenamento, transporte e descarte das informações, sendo uma ferramenta para a prevenção e proteção da informação, pois aponta orientações visando a restrição de acessos e salvaguarda da manipulação por pessoas não autorizadas.

A política de segurança da informação deve ser vista, como um ponto de forte importância e impacto para as empresas, conforme expõem CARUSO e STEFFEN (1999, p. 15) quando reforçam que "... não se deve encarar uma política de segurança como mais um modismo passageiro que freqüentemente aparece em todas as áreas de atividades. Antes de mais nada, política de segurança é um conjunto de diretrizes gerais destinadas a governar a proteção a ser dada a ativos de informação".

Apesar da maioria dos executivos das empresas estarem conscientes da necessidade da criação e cumprimento de uma política de segurança da informação, faz-se necessário um esforço para que estas possam lançar mão dos recursos imprescindíveis para criação e manutenção desta política. Portanto, cumpre identificar os aspectos indicados neste trabalho como sendo os objetivos e a classificação da informação, que oferecem respaldo às discussões desta temática.

4.5.1 Objetivos

Uma política de segurança da informação (TSUNODA, 2003, p. 4), deve prover controles nos ambientes corporativos, quais sejam:

a) *Software* de detecção de vírus e “cavalos de tróia”;

b) s*oftware* de controle de acesso lógico;

c) mecanismos de controle de acesso físico.

Importante destacar, que além de prover controles nos ambientes corporativos, a política de segurança da informação deve estabelecer a distribuição da responsabilidade de todas as áreas envolvidas no manuseio das informações, assim como onde for necessário o atendimento a requisitos específicos e como isso deve ser feito. As pessoas devem estar envolvidas com a proteção das informações, através de conscientização e divulgação para os colaboradores das responsabilidades do seu relacionamento com a informação.

Além disto, a política de segurança da informação, deve envolver os seguintes agentes (TSUNODA, 2003, p. 4):

a) Gestor da Informação - o indivíduo responsável para fazer decisões em nome da organização no que diz respeito ao uso, à identificação, à classificação, e à proteção de um recurso específico da informação.
b) Custodiante - agente responsável pelo processamento, organização e guarda da informação.
c) Usuário - alguma pessoa que interage diretamente com o sistema computadorizado. Um usuário autorizado com poderes de adicionar ou atualizar a informação. Em alguns ambientes, o usuário pode ser o proprietário da informação.

Após o envolvimento dos agentes citados, para garantir que os ativos de informação recebam um nível adequado de proteção, pois a informação possui vários níveis de sensibilidade e criticidade, a informação deve ser classificada para indicar a importância, a prioridade e o nível de proteção desejado.

4.5.2 Classificação da Informação

A informação pode ser classificada conforme o seu grau de sigilo e teor crítico que ela representa para a empresa.

Segundo CARUSO e STEFFEN (1999, p. 29 e 31) “a classificação das informações está subordinada a política de segurança da organização, baseada no valor das informações que estão sendo protegidas e no custo da proteção”. Os autores explicitam, ainda, que analisando-se o valor que a informação representa para a empresa e o seu custo, deve-se avaliar se esta informação deve permanecer sendo considerada como sigilosa ou se a sua importância para a continuidade do negócio ainda é válida, sendo assim, conveniente fazer uma análise de todo o processo de manuseio do fluxo desta informação. Sendo assim, importante a classificação das informações, principalmente pela vulnerabilidade técnica, diversidade humana e as influências externas e/ou internas (CARUSO e STEFFEN, 1999).

Atualmente, a informação é vista como o principal ativo da organização, devendo ser tratada de modo adequado e para isso deve-se classificá-la de acordo com o seu grau de sigilo e seu teor crítico. (LOSS CONTROL, 2001).

Também constata-se em TSUNODA (2003, p. 4), que todo tipo de documento de uma corporação, deve exibir de maneira clara, o respectivo grau de acessibilidade ou seja seu grau de sigilo, o que requer classificar todas as informações segundo o seu grau de criticidade e âmbito de acesso:

a) Informações confidenciais: só podem ser disseminadas para empregados previamente nomeados;
b) informações corporativas: sua divulgação restringe-se ao âmbito da empresa;
c) informações públicas: podem ser disseminadas dentro e fora da empresa.

Ainda em TSUNODA (2003, p. 5), constata-se que a política de segurança da informação precisa contemplar os aspectos tecnológicos, visando as seguintes facetas:

a) Política de acessos externos à Instituição:
   - definição de Convênios para acesso às bases corporativas;
   - criptografia;
   - certificação;
   - *log* de acessos;
   - configuração de *firewall.*

b) Política de uso da Intranet:
   - padrão de *home-page*;
   - padrão de Gerenciamento de Rede;
   - padrão de distribuição de versões de *software*;
   - modelo de identificação de pirataria;
   - detecção e inatividade de *modens* ligados a rede;
   - padrão de atualização de anti-vírus.

c) Política de uso da Internet:
   - acesso de empregados ao provedor corporativo;
   - padronização da *home-page* institucional;
   - padronização da *home-page* comercial;
   - criptografia;
   - certificação;
   - configuração do *firewall*;
   - roteamento;
   - eventos mínimos a serem logados nos sistemas corporativos;
   - trilhas de auditoria;
   - política de *backup*.

d) Política de uso de *software*:
   - controle antipirataria;
   - definição da linha-mestra dos *softwares* utilizados por ambiente
   - computacional.

e) Política de acesso físico:
   - controle de acesso físico;
   - definição de ambientes físicos de alta criticidade;
   - monitoração de ambientes.

f) Política de acesso lógico:
   - política de senhas e de identificação de usuário;
   - definição de perfis de acesso aos ambientes e aplicativos;
   - *log* de eventos mínimos nas transações: dia e hora do acesso, endereço eletrônico de quem acessou, ações executadas.

Considerando-se os aspectos tecnológicos, torna-se importante destacar, que os avanços na área dos computadores, têm permitido a automação de muitos processos e trabalhos antes manuais, em uma variedade de aplicações, em geral com foco no aspecto econômico e relacionado ao aumento da produtividade, na redução dos custos, além de outros objetivos como a redução da fadiga e de tempo em processos repetitivos, precisão no manuseio de informações, etc. Entretanto, os equipamentos de automação agregam um alto valor monetário no processo, como os custos dos equipamentos, dos custos decorrentes da própria operação, manutenção e de treinamento aos operadores; por outro lado, em determinadas aplicações, é necessário a aplicação da redundância nos equipamentos para que os níveis de confiabilidade sejam garantidos (LEVESON, 1997).

Neste particular, as organizações se questionam com relação ao custo a ser investido em tecnologia, para o melhor desenvolvimento e alcance da eficiência e eficácia, pela qual as organizações buscam, como pode-se analisar abaixo:

> Custo ou Investimento? Esse sempre foi o dilema de quem gasta com tecnologia da informação. Pergunte aos diretores de informática e todos garantirão que é impossível viver sem computadores no mundo moderno. E terão razão. Mas, se o computador é um conforto, ele também custa dinheiro. E saber quanto se gasta para manter a estrutura tecnológica é apenas o primeiro passo para avaliar sua eficácia e sua eficiência. Sem isso,

> fica impossível dimensionar se o computador traz ou não o retorno desejado. (GUROVITZ, 2001, p. 40).

Algumas tarefas realizadas por humanos necessitam de precisão de uma máquina eletrônica, mas são os homens que criam as especificações para estas máquinas e muitas destas especificações contêm inconsistências e indefinições (MARTIN, 1991, p. 12). Antigamente, a atenção sobre a segurança da informação estava focada para a tecnologia. Hoje, o desafio é estabelecer efetivamente uma cultura organizacional para que seja possível construir uma relação de confiabilidade com clientes e parceiros.

Confirmando tal tendência, REZENDE e ABREU (2000, p. 18) afirmam que "as empresas estão procurando dar mais atenção ao ser humano, pois é ele que faz com que as engrenagens empresariais funcionem perfeitas e harmonicamente, buscando um relacionamento cooperativo e satisfatório para ambas as partes, com objetivos comuns".

Um dos principais problemas relacionados com as pessoas, nos escopos da segurança da informação, relaciona-se à divulgação das informações não autorizadas pela organização, o que se constitui em uma falta ética e moral grave, pois a divulgação aleatória de dados ou informações organizacionais pode acarretar em perdas econômicas ou em danos quanto à imagem dos produtos e/ou serviços da organização (danos estratégicos). Com base na tradicional pirâmide de níveis dentro de uma empresa (FIGURA 1), o nível operacional é caracterizado por dois lados: quem precisa implantar a segurança e as pessoas que precisam utilizar os recursos da empresa.

FIGURA 1 – Pirâmide tradicional de níveis dentro de uma empresa

Fonte: LAUREANO (2004)

Os negócios de uma organização, conforme REZENDE e ABREU (2000, p. 20), estão atrelados a três itens importantes:

a) Processos: conjunto de atividades que produzem um resultado útil para o cliente interno e externo.
b) Pessoas: grupos que visam alcançar seus objetivos e atender as suas necessidades. Na realidade, são as pessoas que projetam e executam os diversos processos dentro de uma empresa.
c) Tecnologia: toda e qualquer ferramenta utilizada pelas pessoas da empresa para que seja realizada.

A FIGURA 2* demonstra que para atingir a estratégia almejada, a organização deve fazer com que haja interação entre os processos, as pessoas e tecnologias, despertando assim, a conscientização de todas as partes envolvidas.

---

* ***Firewall*** - ("Parede de Fogo") - É um sistema de segurança cujo principal objetivo é filtrar o acesso a uma rede.
PKI - (*Public Key Infrastructure*) - Infra-Estrutura de Chave Pública, é uma tecnologia que objetiva melhorar a segurança das informações.
IDS - (*Intrusion Detection System*) - Sistema de Detecção de Intrusos, é um sistema que objetiva detectar tentativas de ataques.

FIGURA 2 – Conscientização das partes envolvidas para alcançar estratégia proposta pela empresa

Fonte: LAUREANO (2004)

Concentrando-se no eixo “pessoas“ da FIGURA 2, DeMARCO e LISTER (1990, p. 27), afirmam que “os principais problemas de uma empresa não são de natureza tecnológica, mas sim sociológica”. Com base nesta afirmativa, pode-se especular que o elo mais fraco de um processo de segurança é a pessoa (ou grupo de pessoas).

Neste contexto, alguns cuidados devem ser tomados com relação às pessoas, processos e tecnologias de uma empresa (DeMARCO e LISTER, 1990, p. 31):

a) Ensinar aos seus funcionários a ler sobre o desenvolvimento do seu trabalho;
b) é possível obter qualidade sem ferramentas “maravilhosas”;
c) não existe técnicos ou ferramentas que tragam a qualidade de uma hora para outra;
d) constantes modificações são inimigas da qualidade;
e) não construa sistemas que querem prever e tratar as possibilidades altere somente quando um caso raríssimo ocorrer;
f) uma metodologia funciona, quando toda a equipe conhece, entende e compreende o significado da mesma;

g) os melhores testes são feitos por outros técnicos que não participaram da confecção do *software.* Mais importante, os técnicos que realizam os testes conhecem tanto a área de negócio como da área tecnológica.

Todas as informações, ou quase todas, têm interferência de um ser humano no processo ou tecnologia, neste caso é necessário garantir a confiabilidade humana nas partes envolvidas. No contexto da engenharia, por exemplo, segundo LASALA (1998, p. 5) “a confiabilidade humana é a probabilidade de que um humano execute corretamente uma tarefa designada em um tempo especificado, durante um período de tempo definido em um ambiente também especificado”.

Dentro dos aspectos da cultura organizacional, uma política de segurança da informação significa delegar responsabilidades para funcionários, que passam a responder por seus atos (se colaboram para a disseminação de um vírus, por exemplo). A importância da conscientização da equipe de profissionais é consenso entre os especialistas em segurança (BARBOSA, 2001, p. 27). Além disto, de acordo com D`ANDRÉA (2004) “as iniciativas de conscientização dos usuários sobre a segurança da informação podem alavancar vantagem competitiva, desde que a ênfase seja dada às pessoas, à cultura organizacional e aos aspectos de inteligência competitiva”.

Porém, apesar de alguns autores evidenciarem e afirmarem que a cultura organizacional é um elemento fundamental para a prática efetiva de uma política de segurança da informação, ainda assim, a visão de segurança da informação está atrelada ao restrito meio tecnológico, esquecendo que, por trás de cada máquina, há pelo menos uma pessoa. Pensar em segurança da informação é pensar além do aspecto tecnológico, e sim imaginar uma complexa estrutura de pessoas, meios, processos e informações, interagindo de maneira a preservar a confidencialidade, integridade e disponibilidade.

As questões levantadas sobre segurança da informação são inúmeras e complexas. Para tentar sanar as mesmas e solucionar vários problemas relacionados a ISO divulgou, em 01/12/2000, a norma internacional ISO/IEC 17799:2000 (Código de prática para a gestão da segurança da informação). A existência e aplicação de uma norma permite ao usuário tomar conhecimento do quão protegidas e seguras estarão as suas informações, possibilitando ao mesmo uma ferramenta que irá auxiliar a escolha de uma solução. Esta norma, em sua

documentação, aborda dez tópicos pertinentes à segurança da informação considerando tanto os aspectos tecnológicos como os aspectos relativos a cultura organizacional.

4.6 NORMAS TÉCNICAS DE SEGURANÇA DA INFORMAÇÃO

O ser humano sempre se preocupou com a sua segurança e de seus bens, isto faz parte de nossos instintos. Como nos dias atuais, o maior bem que a humanidade possui são as informações e conhecimentos gerados por ela, houve a necessidade do desenvolvimento de métodos e técnicas que permitissem a sua proteção.

Grandes empresas, agências governamentais e instituições internacionais têm trabalhado para estabelecer padrões e normas que reflitam as melhores práticas de mercado relacionados à segurança dos sistemas e informações.

Em 1987, o Departamento de Comércio e Indústria do Reino Unido (DTI) criou um Centro de Segurança de Informações, o CCSC (*Commercial Computer Security Center*). Dentre suas atribuições, existe a tarefa de criar uma norma de segurança das informações para o Reino Unido (MACEDO, 2003, p. 19).

No ano de 1989, foi publicado pelo CCSC a primeira versão desta norma, denominada PD 0003 – Código para gerenciamento de segurança da informação.

No ano de 1995 após vários publicados por esse centro e da revisão do código PD 0003, surgiu o BS7799 (*British Standart* 7799).

A norma BS7799 foi desenvolvida devido ao grande crescimento do *networking* entre as organizações, fato que tornou necessário o gerenciamento de segurança da informação. O objetivo principal desta norma é assegurar a continuidade e diminuir o dano empresarial, prevenindo e minimizando o impacto de incidentes relacionados à segurança. A BS7799 especifica os assuntos necessários para estabelecer um referencial para as organizações desenvolverem, implementarem e avaliarem a gestão da segurança da informação. É baseada em assegurar a integridade, a disponibilidade e a confidencialidade dos recursos incorporados.

No mês de dezembro de 2000, após realização de diversas alterações e sugestões, a BS7799 ganhou *status* internacional com a sua publicação ISO/IEC

17799:2000. A ABNT (Associação Brasileira de Normas técnicas) homologou sua versão brasileira da norma, denominada NBR ISO/IEC 17799.

Há ainda o COBIT (*Control Objectives for Information and Related Technologies*), que pode ser traduzido como Objetivos de Controle para a Informação e Tecnologia relacionada. O COBIT foi publicado pela ISACA (*Information Systems Audit and Control Foundation*) em 1996 e trata-se de uma estrutura para o gerenciamento dos processos de negócios alinhada a um modelo de governança corporativa em Tecnologia da Informação que permite o entendimento e o gerenciamento dos riscos.

Porém, torna-se importante esclarecer que, apesar de existir outras normas e controles relacionados à segurança da informação, como por exemplo o COBIT, o presente trabalho tem como proposta aprofundar a temática tendo como base a NBR ISO/IEC 17799.

4.6.1 O Surgimento da Norma NBR ISO/IEC 17799 (Código de Prática para a Gestão da Segurança da Informação)

Os esforços relacionados com a busca de melhores mecanismos para salvaguardar a segurança culminaram com a homologação da "Norma Internacional de Segurança da Informação" denominada ISO/IEC 17799:2000. Esta norma trata da segurança das informações e não somente dos dados que trafegam pela rede ou que residem dentro de um sistema computacional.

Com base em GONÇALVES (2004) segue em anexo, a citação de um pequeno histórico da mesma (ANEXO 1).

Atualmente, o comitê ISO/IEC JCT1 SC27 é o mantenedor e o responsável pela revisão da ISO/IEC 17799:2000. Devido ao processo de revisão que esta ISO está passando, o comitê recebeu, recentemente, um conjunto de comentários sobre a mesmas, e em 24 de abril de 2003 foi realizado um encontro em Quebec - Canadá, no qual os comentários restantes foram discutidos e uma nova versão da norma foi preparada. A nova versão da ISO/IEC 17799 está prevista para o final do ano de 2004 ou início de 2005.

Contudo, a Norma de Segurança da Informação trouxe mais do que vários controles de segurança. Ela permitiu a criação de um mecanismo de certificação das organizações, semelhante as certificações ISO já existentes. Porém, esta nova certificação "afirma" que a organização certificada manipula os seus dados e os dados dos clientes de forma segura, independentemente da forma como eles estão armazenado.

A Associação Brasileira de Normas Técnicas (ABNT), que é a responsável pelo Fórum Nacional de Normalização, em abril de 2001, disponibilizou para consulta pública o Projeto 21:204.01-010, que daria origem a norma nacional de segurança da informação: NBR ISO/IEC 17799.

A versão final da NBR ISO/IEC 17799, que é uma tradução literal da norma Internacional de Segurança da Informação - ISO/IEC 17799:2000, foi homologada em Setembro de 2001 e sua publicação inclui oficialmente o Brasil no conjunto de países que, de certa forma, adotam e apoiam o uso da norma de Segurança da Informação ABNT2001. E esta versão da NBR ISO/IEC 17799 vem sendo utilizada por vários outros países, como é o caso de Portugal, Angola e outros.

Segundo MACEDO (2003, p. 22-23) os objetivos desta norma são:

a) estabelecer referencial para as organizações desenvolverem, implementarem e avaliarem a gestão da segurança da informação;
b) promover a confiança nas transações comerciais entre as organizações;
c) manter a segurança dos recursos de processamento da informação por prestadores de serviços, controlando o seu acesso;
d) proteger adequadamente os ativos da informação, inventariando-os e alocando uma equipe responsável para cada um;
e) reduzir os riscos de erros humanos, roubo, fraude ou uso indevido das instalações;
f) assegurar que os usuários estejam cientes das ameaças, treinando-os nos procedimentos de segurança e no uso correto das instalações de processamento da informação;
g) prevenir acesso não autorizado às informações e instalações da empresa;
h) minimizar o risco de falhas nos sistemas. Proteger a integridade do *software* e da informação;

i) estabelecer procedimentos de rotina para execução de cópias de segurança e para a disponibilização dos recursos de reserva;
j) garantir a proteção da infra-estrutura de suporte, principalmente do gerenciamento da rede;
k) prevenir a perda, modificação ou mau uso de informações trocadas entre organizações;
l) proteger a confidencialidade, autenticidade ou integridade das informações, garantindo que a segurança seja parte integrante dos sistemas de informação

A norma nacional de segurança de informação é bem abrangente, pretendendo contemplar todos os aspectos da Segurança da Informação. Nesse sentido, divide-se em 10 macros controles, cada qual abordando um aspecto da segurança da informação (NBR ISO/IEC 17799, p. 2-51):

a) **Política de Segurança**: prover orientação e apoio à empresa para a segurança da informação;
b) **Segurança organizacional**: prover infra-estrutura de segurança da informação na organização;
c) **Classificação e controle dos ativos de informação**: manter a proteção adequada dos ativos de informação;
d) **Segurança em pessoas**: reduzir os riscos de erro humano, roubo, fraude ou uso indevido de instalações;
e) **Segurança física e do ambiente**: prevenir acesso não autorizado, dano e interferência às informações e instalações físicas da organização;
f) **Gerenciamento das operações e comunicações**: garantir a operação segura e correta dois recursos de processamento da informação;
g) **Controle de acesso**: controlar o acesso à informação;
h) **Desenvolvimento e manutenção de sistemas**: garantir que a segurança seja parte integrante dos sistemas de informação;
i) **Gestão da continuidade do negócio**: não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos;

j) **Conformidade**: garantir conformidade dos sistemas com as leis, estatutos, regulamentações, obrigações contratuais, políticas e normas organizacionais de segurança e de quaisquer requisitos de segurança.

Cada um destes controles é subdividido em vários outros controles, a NBR possui um total de 137 controles de segurança. Os Controles da norma nacional de segurança visam manter e gerir a segurança da informação nas organização.

No contexto da norma NBR ISO/IEC 17799, é essencial que uma organização identifique as suas necessidades de segurança **antes de implantar qualquer controle**. Existem três fontes principais a serem analisadas:

a) A primeira fonte é obtida a partir da análise de risco da informação. Conforme verificado no item 4.4, pela análise de risco é que são identificadas as vulnerabilidades e ameaças a que a informação está sujeita, bem como a probabilidade de ocorrência. Com isso, pode-se dimensionar o impacto quando da ocorrência dessas falhas;
b) a segunda fonte são a legislação vigente, os estatutos, as regulamentações e as claúsulas contratuais que a organização tem que cumprir;
c) a terceira fonte é o conjunto particular de princípios, objetivos e exigências para processamento da informação que uma organização tem que desenvolver para apoiar suas operações.

A Norma aconselha, ainda, a listar todos os controles e identificar aqueles considerados ideais para a análise de risco, realizando assim, a declaração de aplicação que deverá responder qual o objetivo da empresa, e esta declaração, por sua vez, servirá como métrica para responder até onde se conseguiu chegar.

Torna-se imprescindível a criação de um documento de gestão. Este será um guia de referência à continuidade do processo de segurança, visto que, a cada novo processo inserido ao negócio, deverá ser obrigatoriamente avaliado e protegido conforme um modelo padrão.

Segundo MACEDO (2003, p. 26) “é possível obter-se certificação através de auditoria realizada por uma certificadora, de forma muito parecida com o da ISO 9000, se for seguido alguns requisitos mínimos, tais como: Plano de Gestão de Segurança da Informação; Criação de uma Coordenação de Segurança da Informação; e Administração e Controle dos Processos”.

Essas auditorias têm o objetivo de avaliar a eficiência e eficácia das práticas adotadas na organização. Seus pontos fundamentais são: Análise de Riscos (revisão da documentação frente as mudanças na organização) e Declaração de Aplicação (documento que deve ser revisado em curtos intervalos de tempo).

Os benefícios obtidos através da NBR ISO/IEC 17799, são explicitados pela *Empresa Módulo Security,* a qual defende que, com a adoção da Norma, a organização pode fazer mais negócios do que aquelas que não seguem um padrão. E ainda comentam que, se um cliente em potencial estiver escolhendo entre dois serviços diferentes, e a segurança for uma preocupação, eles geralmente selecionarão àquela que seguir determinado padrão na área.

Citam também, que uma empresa que segue o padrão NBR ISO/IEC 17799 oferecerá:

a) Segurança corporativa aprimorada;
b) planejamento e Gerenciamento de segurança mais efetivo;
c) parcerias e *e-commerce* mais seguros;
d) confiança aprimorada do cliente;
e) auditorias de segurança mais seguras e precisas;
f) redução de responsabilidades legais .

A *Empresa Módulo Security* adverte que se a empresa não possui um programa de proteção de informações, a NBR ISO/IEC 17799 pode fornecer as diretrizes para a criação de um. Mesmo que a empresa não queira se tornar certificada, a NBR ISO/IEC 17799 pode servir como um guia para a criação da postura de segurança da informação da empresa. Pode-se até pensar nesse padrão como uma diretriz de segurança a ser usada pelas empresas. Porém, a empresa poderá descobrir que os benefícios da certificação podem ser muito abrangentes.

Percebe-se, portanto, que as discussões no âmbito de segurança da informação apresentam-se de forma contínua. Prova disto são as Pesquisas Nacionais de Segurança da Informação, promovidas pela *Empresa Módulo Security,* que têm acontecido anualmente desde 1995, acompanhando a evolução da temática iniciada no Brasil nos anos 90.

4.7 PESQUISA NACIONAL DE SEGURANÇA DA INFORMAÇÃO

Pelo nono ano consecutivo, a *Empresa Módulo Security*, empresa brasileira especializada em tecnologia de segurança da informação, desenvolveu a 9ª Pesquisa Nacional sobre Segurança da informação, visando fornecer dados estatísticos atualizados sobre o mercado brasileiro. Entre março e agosto de 2003, a pesquisa quantitativa coletou uma amostra de 682 questionários (com respostas presenciais e *online*), junto a profissionais ligados às áreas de Tecnologia e Segurança da Informação.

Os resultados obtidos reforçam a importância dos fatores de capacitação e conscientização como pontos fundamentais para proteção das informações corporativas, além de demonstrar o estado da arte e as novas tendências relacionadas à área.

Os profissionais que participaram deste estudo estão distribuídos em diversos segmentos, como: ***Financeiro (21%), Governo (17%), Indústria e Comércio (14%), Tecnologia/Informática (14%), Prestação de Serviços (9%), Outros (8%), Telecomunicações (7%), Comércio/Varejo (4%), Energia Elétrica (2%), Educação (2%) e Saúde (2%)***, correspondendo a cerca de 50% das 1000 maiores empresas brasileiras.

Alguns dos principais destaques, dos resultados obtidos com esta 9ª Pesquisa Nacional de Segurança da Informação, foram:

a) 42% das empresas tiveram problemas com a Segurança da Informação nos seis meses anteriores à pesquisa e 35% das empresas reconhecem que tiveram perdas financeiras em função destes problemas;
b) Vírus (66%), funcionários insatisfeitos (53%), divulgação de senhas (51%), acessos indevidos (49%) e vazamento de informações (47%) foram apontados como as cinco principais ameaças à segurança das informações nas empresas;
c) A falta de consciência dos executivos é apontada por 23% dos entrevistados como principal obstáculo para implementação da segurança;
d) 63,5% dos entrevistados adotam a NBR IEC/ISO 17799 como a principal norma que norteia suas empresas;

e) Política de Segurança da Informação formalizada já é realidade em 68% das organizações, porém apenas 21% das empresas afirmaram possuir um Plano de Continuidade de Negócios (PCN) atualizado e testado; e 48% não possuem nenhum plano de ação formalizado em caso de invasões e ataques (internos e externos);
f) A área de Tecnologia (49,5%) continua sendo a principal responsável pelo gerenciamento da Segurança da Informação nas empresas, seguida pela área específica, *Security Office*, com 25,5%;
g) Pelo terceiro ano consecutivo, antivírus (90%), sistemas de *backup* (76,5%) e *firewall* (75,5%) foram apontados como as três medidas de segurança mais implementadas nas empresas;
h) 60% afirmam que os investimentos de suas empresas em Segurança para 2004 vão aumentar.

Teoricamente, a Segurança da Informação está embasada em duas escolas: a escola técnica (aspectos tecnológicos) e a escola não-técnica (aspectos culturais), porém apesar de vários autores ressaltarem a importância dessas duas escolas, ainda hoje, conforme verificado nos dados citados acima, as empresas fixam-se nos aspectos tecnológicos que envolvem o tema e continuam citando, de maneira superficial, os aspectos envolvendo cultura organizacional.

Um dos mais importantes resultados desta pesquisa é o que trata da adequação com legislação, regulamentação e normas. Este estudo mostra que por um lado a ISO/IEC 17799 tem sido adotada fortemente como referência técnica pelas equipes de Segurança da Informação, seguida pelo COBIT[4], muitas vezes em conjunto. Mas, por outro lado, cada segmento tem também adotado as regulamentações específicas como por exemplo, resoluções do banco Central e decretos do Governo Federal.

A 9ª Pesquisa revela o **fortalecimento** da NBR ISO/IEC 17799 como a principal norma para implementação da Gestão em Segurança da Informação, complementando outras normas, legislações e regulamentações que já vinham sendo utilizadas pelas organizações. Tudo isso tem se destacado como uma oportunidade para os profissionais de Segurança da Informação nos próximos anos,

[4] **COBIT** – *Control Objectives for Information and Related Technologies*.

uma vez que a matéria se aproxima a cada dia da sua atividade-fim e dos executivos da organização.

De acordo com os dados obtidos na 9ª Pesquisa Nacional de Segurança da Informação, a nível nacional, a temática envolvendo segurança da informação está em crescente ascensão.

As pesquisas de âmbito nacional, tais como a descrita acima, disponibilizam um estado da arte sobre o tema. Contudo, estudos mais específicos podem, igualmente, explorar aspectos diferenciados em diferentes tipos de organizações. O presente trabalho explora a grande área de Segurança da Informação voltada, todavia, para as empresas de grande porte situadas no município de Curitiba.

5 METODOLOGIA

A presente pesquisa seguiu alguns procedimentos metodológicos, tais como: referencial teórico, estruturação das questões de pesquisa, elaboração e aplicação do instrumento de coleta (questionário), análise dos dados coletados, considerações finais e sugestões de continuidade.

A pesquisa teve caráter **exploratório** e, primeiramente, no referencial teórico foram abordados aspectos gerais relacionados à segurança da informação. Além do caráter exploratório este estudo também apresenta características de uma pesquisa **bibliográfica**, pois a mesma foi baseada a partir de material já elaborado: livros, artigos científicos, *sites* de Internet e a própria NBR ISO/IEC 17799.

Paralelamente, foi realizado um **levantamento de dados**, pois para identificar informações pertinentes tornou-se necessário perguntar, diretamente ao universo especificado, às condições relativas a realidade em que a temática se insere.

Para identificar o universo desejado, consultou-se a Federação das Indústrias do Estado do Paraná (FIEP), utilizando-se do instrumento de busca **Catálogo Industrial do Paraná/2004** (ANEXO 2). O universo do estudo compreendeu as empresas de grande porte, de diferentes setores de atuação, do município de Curitiba (ANEXO 3), resultando em um total de 25 (vinte e cinco) empresas. Este total reduziu-se para 22 empresas, pois uma empresa apresentada

divide-se em quatro unidades com CNPJ próprio ainda que para todas exista apenas um único setor responsável pela Segurança da Informação, portanto esta empresa foi considerada uma única vez.

O critério utilizado na seleção destas empresas baseou-se na classificação por tamanho da empresa, adotada pelo Serviço de Apoio às Micros e Pequenas Empresas (SEBRAE), como indica o QUADRO 1.

QUADRO 1 – CLASSIFICAÇÃO POR TAMANHO DA EMPRESA

Número de Empregados	Tamanho da Empresa
1 – 19	Micro
20 – 99	Pequena
100 – 499	Média
Acima de 500	Grande

Fonte: SEBRAE (2004)

Após a posse da listagem, com a relação das empresas selecionadas, foi realizado contato telefônico, para que fosse possível expor os objetivos do proposto trabalho e verificar a disponibilidade das empresas em participar da pesquisa. Independente da empresa contatada, quando explicado que o assunto de interesse era segurança da informação, todas as ligações foram encaminhadas ao setor de informática das empresas.

Como instrumento para a técnica de coleta de dados, elaborou-se um **questionário** contendo 10 questões fechadas, pois conforme verificou-se em CERVO (1983, p. 160) “as perguntas fechadas são padronizadas, de fácil aplicação, fáceis de codificar e analisar”.

O questionário foi elaborado segundo os objetivos determinados neste estudo, assegurando sigilo aos entrevistados, e antes do início do mesmo, para efeito de esclarecimento, incluiu-se um texto sucinto de apresentação.

Realizou-se um pré-teste para a verificação da validade do questionário. Ao serem contatadas, via contato telefônico, cinco empresas concordaram em avaliar o instrumento de coleta (seguindo os critérios citados a seguir) e reenviá-lo via *e-mail*.

Os critérios de avaliação do questionário foram apoiados em GIL (1996, p. 96). Portanto aos participantes do pré-teste solicitaram-se considerações sobre:

a) Clareza e precisão dos termos:
b) quantidade de perguntas;
c) forma das perguntas;
d) ordem das perguntas;
e) introdução (texto explicativo do início do questionário).

Das cinco empresas que participaram do pré-teste apenas uma não enviou seus comentários. A partir dos comentários enviados foram realizadas pequenas modificações na primeira e na última questão.

Simultaneamente, enquanto reajustava-se o instrumento de coleta, o restante das empresas foi contatado, via contato telefônico, para verificar se tinham interesse em participar da proposta pesquisa.

Das 22 empresas contatadas, 19 empresas aceitaram participar da proposta pesquisa, demonstrando interesse e disponibilidade em responder o questionário via *e-mail*, 3 empresas não aceitaram participar alegando como motivo a indisponibilidade de tempo.

Após o pré-teste e adaptações feitas ao instrumento de coleta, a versão final do questionário (ANEXO 4) foi enviada para as 19 empresas que compõem a amostra final. Deste total, 10 questionários foram devolvidos devidamente respondidos, representando 53% da amostra. Com base nas respostas obtidas, tornou-se possível confeccionar gráficos e tabelas, realizando-se assim, a descrição dos dados. A partir disto, foi realizada uma análise crítica da descrição dos dados obtidos, e comparando-os às questões de pesquisa e as indicações dos autores que constam no referencial teórico.

6 DESCRIÇÃO E ANÁLISE DOS DADOS

A análise dos dados apresentada abaixo se refere ao total de questionários devolvidos (**10 questionários**). Cada questão foi analisada em ordem seqüencial do questionário.

A **primeira questão**, relacionada à visão geral da empresas sobre segurança da informação (TABELA 1): 30% dos respondentes demonstraram identidade com a definição fornecida pela NBR ISO/IEC 17799; 70% optaram pela definição fornecida no *site* do Bradesco; e nenhum respondente optou pela definição de Lasala que aborda os aspectos relacionados à cultura organizacional (escola não técnica). Conforme é demonstrado, nenhum respondente propôs-se a definir o que sua empresa entende por segurança da informação. O conjunto de respostas obtidas junto a este universo de respondentes leva a crer que há maior tendência a definir segurança da informação no âmbito tecnológico. Por mais que alguns autores, tais como DeMARCO e LISTER (1990, p. 27 e 31) e REZENDE e ABREU (2000, p. 20), evidenciem que é necessária a conscientização de todas as partes envolvidas (processos, tecnologia e pessoas) para que se consiga atingir determinado objetivo da empresa, a resposta dada pelo universo final (empresas efetivamente entrevistadas) reflete que quando trata-se de segurança da informação tende-se a escolher a definição que aborda somente a descrição do processo de segurança maneira ampla, e que sutilmente demonstra preocupar-se com questões de nível tecnológico (presente na definição mais votada pelos entrevistados).

TABELA 1 – DEFINIÇÃO DE SEGURANÇA DA INFORMAÇÃO

Autor	Freqüência	%
NBR ISO/IEC 17799	3	30
BRADESCO	7	70
LASALA	0	0
Definição da própria empresa	0	0
Nenhuma	0	0
Total	**10**	**100**

Fonte: Coleta de dados junto às empresas de grande porte do município de Curitiba (out. 2004).

Na **questão dois**, foram dispostas algumas razões de concordância considerando-se a frase "a segurança da informação é fonte de vantagem competitiva". As razões, apontadas em ordem de importância foram (TABELA 2): a garantia da **integridade** da informação com 40% dos respondentes apontando esta razão em **primeiro lugar**; a garantia da **disponibilidade** da informação com 40% dos respondentes apontando esta razão em **segundo lugar**; a garantia da **confidencialidade** da informação 40% dos respondentes apontando esta razão em **terceiro lugar**; e outros aspectos com 100% dos respondentes apontando em último lugar.

Apesar da tentativa de hierarquizar as razões acima, não é possível afirmar realmente qual dentre elas é apontada como a mais importante, pois embora **integridade** esteja em primeiro lugar com 40%, analisando os três aspectos em conjunto, a diferença percentual entre eles foi mínima.

DRUCKER (1993, p. 25) enfatiza que "a informação e o conhecimento são a chave da produtividade e da competitividade", portanto torna-se imprescindível garantir a integridade, disponibilidade e confidencialidade dos mesmo. Reforçando-se assim, que quem dispõe de informação de boa qualidade, fidedigna, em quantidade adequada e no momento certo, adquire vantagens competitivas mas a falta ou perda de informação dá margem a erros e a perda de oportunidades.

TABELA 2 – SEGURANÇA DA INFORMAÇÃO COMO FONTE DE VANTAGEM COMPETITIVA: RAZÕES DE CONCORDÂNCIA

ORDEM DE IMPORTÂNCIA	
Primeiro Lugar	Garantia da confidencialidade da informação - 30% Garantia da integridade da informação - 40% Garantia da disponibilidade da informação - 30% Outro - 0%
Segundo Lugar	Garantia da confidencialidade da informação - 30% Garantia da integridade da informação - 30% Garantia da disponibilidade da informação - 40% Outro - 0%
Terceiro Lugar	Garantia da confidencialidade da informação - 40% Garantia da integridade da informação - 30% Garantia da disponibilidade da informação - 30% Outro - 0%

Fonte: Coleta de dados junto às empresas de grande porte do município de Curitiba (out. 2004).

Já em relação às razões de discordância, considerada a frase “a segurança da informação é fonte de vantagem competitiva”, as razões apontadas na **questão três** em ordem de importância foram (TABELA 3): os altos **custos envolvidos** com 70% dos respondentes apontando esta razão em **primeiro lugar**; dificuldade de **envolvimento dos funcionários** (questão não técnica) com 80% dos respondentes apontando esta razão em **segundo lugar**; **desconhecimento do assunto** no ambiente da empresa com 90% dos respondentes apontando esta razão em **terceiro lugar**; e outros aspectos com 100% dos respondentes apontando em último lugar.

Interessante como a questão humana ainda é vista, pelas empresas, como um empecilho dentro de segurança da informação, pois o **envolvimento dos funcionários** é apontado em segundo lugar pelos entrevistados com uma porcentagem significativa de 80%.

Apesar de vários autores evidenciarem o fator humano, tais como MARTIN (1991, p. 12), REZENDE e ABREU (2000, p. 20) e BASTOS (2004), e afirmarem que as empresas estão procurando dar mais atenção a este aspecto (não técnico) que envolve a temática abordada, confirmou-se que ainda a grande preocupação das empresas está focada nas questões objetivas, isto é, nos altos custos que envolvem os aspectos tecnológicos. Na 9ª Pesquisa Nacional de Segurança da Informação da *Empresa Módulo Security*, os entrevistados afirmaram que os investimentos em Segurança iriam aumentar em 2004, esta preocupação com relação aos custos pode também estar explicitada nos 70% dos respondentes que apontaram custos em primeiro lugar.

TABELA 3 – SEGURANÇA DA INFORMAÇÃO COMO FONTE DE VANTAGEM COMPETITIVA: RAZÕES DE DISCORDÂNCIA

ORDEM DE IMPORTÂNCIA	
Primeiro Lugar	Altos custos envolvidos - 70% Envolvimento funcionários - 20% Desconhecimento do assunto – 10% Outro - 0%
Segundo Lugar	Altos custos envolvidos - 20% Envolvimento funcionários - 80% Desconhecimento do assunto – 0% Outro - 0%
Terceiro Lugar	Altos custos envolvidos - 10% Envolvimento funcionários - 0% Desconhecimento assunto - 90% Outro - 0%

Fonte: Coleta de dados junto às empresas de grande porte do município de Curitiba (out. 2004).

Verificou-se no decorrer do referencial teórico que, para implementar um programa de segurança da informação, é fundamental que tanto os aspectos tecnológicos quanto os aspectos relacionados a cultura organizacional sejam levados em consideração. DIAS (2000, p. 4) destacou que para implementar um programa de segurança da informação é aconselhável responder algumas questões chaves que envolvem o tema. Portanto, com a pretensão de verificar se o assunto está realmente sendo discutido nas empresas, foi especulado quais as principais questões que estão sendo alvo de discussão nas empresas.

A **questão quatro** levantou os seguintes dados: 50% dos respondentes assinalaram todas as questões citadas no questionário; os outros 50% apontaram no mínimo quatro questões; dentre todas a questão “quais as conseqüências para a instituição se seus sistemas e informações forem violados ou roubados?” foi assinalada por 90% dos respondentes, o que demonstrou novamente que os entrevistados preocupam-se com a questão da **integridade** (conforme questão 2).

Diante dos dados coletados, com base nas questões levantadas por DIAS (2000, p. 4), tornou-se possível especular que as empresa que participaram da pesquisa identificam o tema como relevante e estão discutindo os aspectos mais amplos da segurança da informação no seu ambiente organizacional.

A **questão cinco** procurou expor quais objetivos relativos à segurança da informação seriam mais valorizados pelas empresas. A TABELA 4 apresenta os três objetivos considerados mais importantes pelos respondentes.

Importante comentar que, se analisados em separado, a **Integridade dos dados** foi apontada 80% das vezes dentre um dos objetivos mais importantes da segurança da informação, **Confidencialidade**/**Privacidade** foi apontada 60% das vezes e **Disponibilidade** foi apontada 50% das vezes.

Interessante destacar que a NBR ISO/IEC 17799 (2001, p. 4) cita que a segurança da informação é caracterizada pela preservação, justamente, da confidencialidade, integridade e disponibilidade, isto é, dos mesmos objetivos que foram os mais apontados pelos respondentes.

TABELA 4 – OBJETIVOS VALORIZADOS RELACIONADOS À SEGURANÇA DA INFORMAÇÃO.

OBJETIVOS VALORIZADOS	
Confidencialidade/privacidade; Integridade de dados; Disponibilidade	20%
Confidencialidade/privacidade; Integridade de dados; Confiabilidade	20%
Confidencialidade/privacidade; Legalidade; Auditoria	10%
Confidencialidade/privacidade; Integridade de dados; Isolamento ou uso ilegítimo	10%
Integridade de dados; Disponibilidade; Confiabilidade	30%
Confidencialidade/privacidade; Legalidade; Isolamento ou uso ilegítimo	10%
Prefiro não opinar	0%
TOTAL	100%

Fonte: Coleta de dados junto à empresas de grande porte do município de Curitiba (out. 2004).

A **questão seis** abordou os mecanismos técnicos utilizados nas empresas para garantir a segurança da informação. Considerando-se os resultados obtidos (TABELA 5) 40% dos respondentes optaram por escolher todos os mecanismos citados; 20% preferiram não opinar sobre a questão e as porcentagens restantes demostram que os respondentes optaram pela combinação diferenciada dos mecanismos citados ou que optaram por apenas um dos mecanismos.

Em uma análise, em separado, **Senhas fortes** foi o mecanismo apontado por 80% dos entrevistados. Destaca-se que este é um dos mecanismos técnicos mais utilizados para garantir a segurança da informação. Esta preocupação das

empresas em possuir senhas fortes, refletiu-se também nos resultados 9ª Pesquisa Nacional de Segurança da Informação, pois as principais ameaças apontadas à segurança das informações das empresas foram: Vírus (66%), funcionários insatisfeitos (53%), divulgação de senhas (51%), acessos indevidos (49%) e vazamento de informações (47%).

TABELA 5 – MECANISMOS TÉCNICOS UTILIZADOS NAS EMPRESAS

MECANISMOS TÉCNICOS	
Senhas fortes	10%
Manuseio técnico adequado	0%
Investimento em TI	0%
Outros mecânismos técnicos	0%
A empresa não utiliza de quaisquer mecanismos	0%
Prefiro não opinar.	20%
Senhas fortes e Investimento em TI	10%
Senhas fortes e Outros mecanismos técnicos	10%
Senhas fortes; Manuseio técnico adequado; Investimento em TI	40%
Manuseio técnico adequado e Investimento em TI	10%
TOTAL	100%

Fonte: Coleta de dados junto às empresas de grande porte do município de Curitiba (out. 2004).

Com relação aos aspectos não tecnológicos envolvidos com a segurança da informação, a **questão sete** (TABELA 6) demonstra que 80% dos respondentes consideram a existência de uma política de segurança da informação como o aspecto mais importante, seguido de 10% dos respondentes que optaram pelo comprometimento contínuo dos funcionários, e outros 10% preferiram não opinar sobre a questão.

No decorrer do referencial teórico foi exposto que, pensar em segurança da informação é pensar além do aspecto tecnológico, é imaginar uma complexa estrutura de pessoas, meios, processos e informações, interagindo de maneira a preservar a confidencialidade, integridade e disponibilidade.

A NBR ISO/IEC 17799 (2000, p. 2) destaca que a segurança da informação alcança por meios técnicos é limitada e convém que a mesma seja apoiada por gestão e procedimentos apropriados, contando com a participação de todos os funcionários da organização. Entretanto, no sentido de TSUNODA (2003, p. 4) uma política de segurança da informação tende a direcionar-se para escola técnica, deixando a escola não técnica em segundo plano. Talvez a visão dos entrevistados esteja de acordo com a visão de TSUNODA, uma vez que os pontos relativos à pessoas (funcionários) foram mais fracamente votados.

TABELA 6 – ASPECTOS NÃO TECNOLÓGICOS RELACIONADOS À SEGURANÇA DA INFORMAÇÃO

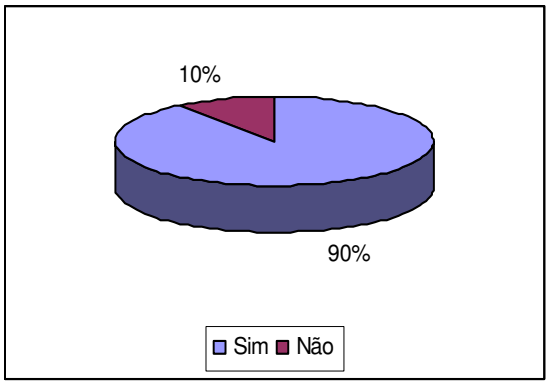
ASPECTOS NÃO TECNOLÓGICOS	
Existência de uma política de segurança da informação	80%
Comprometimento contínuo dos funcionários	10%
Esclarecimento dos funcionários	0%
Outros	0%
Prefiro não opinar	10%
TOTAL	100%

Fonte: Coleta de dados junto às empresas de grande porte do município de Curitiba (out. 2004).

Com relação aos procedimentos segurança da informação nas empresas, verificou-se que o custo é um fator relevante, pois na **questão oito** 90% dos respondentes confirmaram tal afirmação e apenas 10% negaram, conforme demonstram os dados coletados no GRÁFICO 1.

Já com relação aos custos envolvidos, parece comprovado pelos respondentes a pressão da escola técnica (equipamentos, software, etc.), pois destes 90% que afirmaram que o custo nestes aspectos é um fator relevante. Por outro lado, 30% dos respondentes assinalaram todas as alternativas e 30% dos respondentes apontaram o custo dos softwares e contratação de especialistas/consultores como relevante. O custo dos equipamentos e custo dos softwares representou 10% das respostas, enquanto 20% dos respondentes preferiu não opinar e 10% dos entrevistados não responderam a questão.

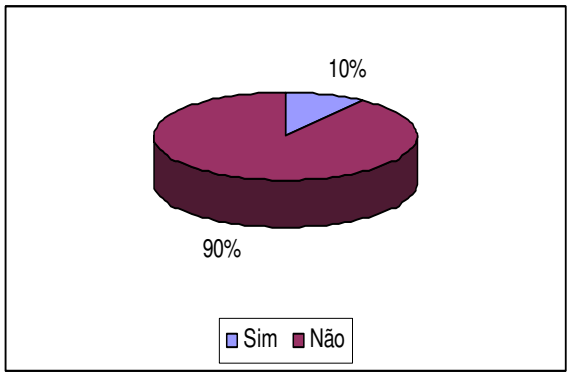
GRÁFICO 1 – VERIFICAÇÃO DA RELEVÂNCIA DOS CUSTOS ENVOLVIDOS NOS PROCEDIMENTOS EM SEGURANÇA DA INFORMAÇÃO



Fonte: Coleta de dados junto às empresas de grande porte do município de Curitiba (out. 2004).

Na **questão nove** perguntou-se se as empresas aplicavam a NBR ISO/IEC 17799. Constatou-se que apenas 10% dos respondentes, o que corresponde a **uma empresa**, aplicam efetivamente a Norma e 90% não a aplicam (GRÁFICO 2).

GRÁFICO 2 – APLICAÇÃO DA NBR ISO/IEC 17799 NAS EMPRESAS SELECIONADAS



Fonte: Coleta de dados junto às empresas de grande porte do município de Curitiba (out. 2004).

Dos entrevistados que responderam a **questão dez**, 10% dos respondentes (esta porcentagem eqüivale à única empresa que aplica efetivamente NBR ISO/IEC 17799) marcaram **todos os itens** abordados pela Norma. Entretanto, um fator interessante é que apesar da maioria ter afirmado não aplicar a Norma, quando responderam a **questão dez** 20% destes respondentes apontaram itens da norma que estão sendo incrementados em suas empresas, tais como: **Conformidade**

representando 10% dos entrevistados e **Segurança Organizacional** também representando 10%. Portanto, mesmo não aplicando efetivamente a Norma, as empresas entrevistadas revelaram que questões relativas à segurança da informação estão realmente sendo discutidas em seus ambientes organizacionais (conforme verificado, também, na **questão quatro**).

7 CONSIDERAÇÕES FINAIS

Na elaboração desse trabalho constatou-se que o tema “segurança da informação” é o elemento chave dentro da organização contemporânea: envolve aspectos técnicos, humanos e organizacionais, sendo fundamental a definição e existência de um política para efetiva proteção das informações.

A pesquisa evidenciou, minimamente para a amostra investigada, que a informação é considerada como um dos principais patrimônios da organização, devendo ser tratada e protegida nos seus aspectos de disponibilidade, integridade, confidencialidade. Segurança da informação é responsabilidade e dever de todos e, como tal, deve ser de conhecimento de cada profissional da empresa o cumprimento e conscientização de medidas de proteção dos recursos da informação, pois se trata de questão de alta prioridade.

Percebe-se que a implementação das principais práticas de segurança da informação na organização não é uma tarefa fácil, pois envolve integração de fatores objetivos (técnicos) e subjetivos (não técnicos).

Apesar do estudo não pretender generalizar nas conclusões com relação à temática proposta, devido à amostra investigada, as observações feitas são válidas e retratam a realidade das empresas de grande porte do município de Curitiba.

Verificou-se na **questão quatro**, do instrumento de coleta de dados, que pelo menos 50% dos entrevistados estão discutido os aspectos mais amplos da segurança da informação no seu ambiente organizacional. Porém, tem sido comum a postura de tratar a segurança da informação como um "problema técnico". Em contato telefônico com o universo selecionado, a pesquisadora comprovou que o fluxo de decisão, relacionado a esta temática, acaba geralmente parando nas mãos do Diretor de Informática ou Tecnologia da Informação, que toma as medidas

necessárias sobre o assunto. Esta é uma visão que está diretamente relacionada com a forma de tratamento que o assunto segurança da informação recebe, ou seja, na realidade muitos executivos ainda tratam o assunto como uma questão meramente tecnológica, e não como um diferencial competitivo que envolve também aspectos relacionados à cultura organizacional. É uma estratégia que pode até trazer seus resultados, mas se a segurança da informação for vista como fator de sucesso e garantia de manutenção no negócio, que envolve tanto aspectos técnicos quanto aspectos não técnicos, os ganhos podem ser maiores.

Interessante expor que apesar de vários autores (MARTIN, REZENDE e ABREU, BASTOS, dentre outros) apontarem para a necessidade de envolver os usuários no processo de segurança da informação, a própria NBR ISO/IEC 17799, considerada a melhor referência hoje em termos de práticas para gestão de segurança da informação, pouco fala sobre o processo de **conscientização de usuários**. A necessidade está lá, mas falta detalhamento e direcionamento sobre como isso deve ser feito, tanto que **envolvimento dos funcionários** foi apontado, em segundo lugar, por 80% dos entrevistados (**questão três**) como uma das razões que dificultam tornar segurança da informação em vantagem competitiva.

Outro ponto importante a ser destacado é que em tempos de “economia nervosa”, como os que estamos vivendo, a **racionalização dos investimentos** nas empresas é fundamental. É preciso focar a utilização dos recursos naquilo que mais agrega valor ao negócio. Muitos executivos precisam de números precisos para tomar decisões financeiras, porém em termos de segurança da informação nem sempre isso é possível, já que trabalha-se com a probabilidade da ocorrência de um acidente. Esta preocupação financeira está refletida nos dados coletados nas **questões três e oito**, onde foi comprovado que o **custo** é considerado um fator relevante pelo universo investigado.

A análise dos dados revelou que as empresas de grande porte do município de Curitiba, estão cientes sobre a importância da segurança da informação, porém retratou que ainda esta questão é focada, em sua maioria, dentro dos aspectos técnicos. Por outro lado, mesmo que de maneira superficial, os aspectos não técnicos têm um lugar de discussão, o que se comprova pelos dados coletados na **questão três e sete**.

Considerando as diferentes facetas relacionadas à temática, e levando-se em consideração o que foi levantado no decorrer do trabalho, as questões de pesquisa voltam a ser discutidas.

A **primeira questão de pesquisa** foi confirmada parcialmente, pois foi comprovado que, da amostra estudada, apenas uma empresa de grande porte do município de Curitiba aplica efetivamente a NBR ISO/IEC 17799. As empresas respondentes que não aplicam a Norma, estabeleceram procedimentos relacionados à segurança da informação. Esta preocupação está explicitada na **questão quatro** conforme comentado anteriormente, na **questão seis** onde 40% dos respondentes apontaram todos os mecanismos técnicos (senhas fortes, manuseio técnico adequado e investimento em TI) para garantir a segurança da informação em seu ambiente organizacional e na **questão dez**, pois mesmo não aplicando a Norma a coleta de dados demonstrou que 20% dos entrevistados estão focados em duas áreas específicas que envolvem a segurança da informação (Conformidade e Segurança Organizacional).

Conforme consta no referencial teórico, MOREIRA (2001, p. 11-12) e DIAS (2000, p. 56) comentam que uma vez que as ameaças e as vulnerabilidades no mundo empresarial tendem a crescer, representando riscos para a proteção das informações estratégicas, torna-se uma exigência global que as empresas possuam procedimentos de segurança. Com a conscientização da importância em adotar procedimentos relacionados à segurança da informação as empresas podem:

a) Viabilizar aplicações e processos que otimizem as atividades da empresa, reduzindo custos;
b) viabilizar novos produtos e serviços, aumentando a receita da empresa;
c) reduzir e administrar os riscos do negócio;
d) fortalecer a imagem da empresa (credibilidade);
e) criar valor para a empresa e para os funcionários.

Por outro lado, a ausência de procedimentos de segurança da informação pode acarretar diversos impactos, que levarão a perda de faturamento, custos e despesas e, no final das contas, perda de valor da empresa.

A **segunda questão de pesquisa** foi confirmada, pois através da **questão oito** as empresas entrevistadas revelaram que o custo de implantação

(equipamentos, *softwares*, contratação de especialistas/consultoria, etc.) pode ser um empecilho para a aplicação de procedimentos de segurança da informação. Na **questão três**, as empresas entrevistas, também explicitaram que o **custo** é uma das razões que dificultam tornar a segurança da informação em vantagem competitiva, com 70% dos respondentes apontando esta razão em primeiro lugar.

Mesmo os autores LASALA (1998, p. 5), BARBOSA (2001, p. 27) e D'ANDRÉA (2004) afirmando que pensar em segurança da informação é pensar além do aspecto tecnológico, é imaginar uma complexa estrutura de pessoas, processos e tecnologia, a **terceira questão de pesquisa** também foi confirmada.

No referencial teórico, BASKERVILLE e SIPONEN (2002, p. 337) destacam a existência de duas escolas (técnica e não técnica) em segurança da informação, porém as empresas investigadas continuam vinculando a temática à área técnica e deixam num segundo plano os aspectos relacionados a cultura organizacional, conforme dados já comentados da **questão três**. Outro aspecto interessante na análise dos dados coletados, e que também recaí sob o aspecto tecnológico, é que a **Integridade** sempre é apontada pelos entrevistados com alguma vantagem percentual, como no caso das **questões dois e cinco**, ou aparece de maneira não explícita, como na **questão quatro** onde a frase mais assinalada por 90% dos entrevistados ("quais as conseqüências para a instituição se seus sistemas e informações forem violados ou roubados?") está relacionada com **integridade**, pois conforme a definição da NBR ISO/IEC 17799 (2001, p. 4) "integridade é a salvaguarda da exatidão e precisão da **informação** e dos **métodos de processamento**".

Apesar de existir, na amostra estudada, um predomínio da área de Informática nos processos relativos à segurança da informação, a pesquisadora acredita que à medida que a unidade responsável pela segurança da informação adquire maturidade na sua gestão, e que as atividades informais de proteção dos ativos informacionais vão sendo substituídas por processos planejados, controlados e mensurados (política de segurança da informação), torna-se mais fácil atuar preventivamente levando em consideração os dois aspectos (técnicos e não técnicos) que envolvem a segurança da informação.

A pesquisadora observou que dentro deste contexto de segurança da informação, mesmo existindo o predomínio da área de Informática, o Gestor da

Informação poderá assumir um papel significativo nos processos de planejamento estratégico, colaborando na construção de cenários e na identificação das melhores soluções para a organização não só do ponto de vista do atendimento às suas demandas por informação, mas também para a proteção desse que já é o principal ativo das organizações.

Os objetivos propostos nesta pesquisa foram atingidos. Porém, o reconhecimento das limitações deste estudo em particular, tanto pela ampla extensão que a temática aborda, como do número de retorno dos questionários, leva a sugerir que novos trabalhos possam aprofundar o referido tema, como por exemplo, explorar a utilização dos macro controles da NBR ISO/IEC 17799 e também a utilização de outras normas relacionadas à segurança da informação nas organizações. Estudos sistemáticos nesta temática poderão oferecer um panorama mais nítido e abrangente da área.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17799:** tecnologia da informação – código de prática para a gestão da segurança da informação. Rio de Janeiro, 2001. p. 2–51.

BARBOSA, A. E-business com segurança. **Revista Internet Business**. São Paulo, ano 5, n. 49, p. 27, set. 2001.

BASKERVILLE, R.; SIPONEN M. An information security meta-policy for emergent organizations. **Logistics Information Management.** v. 15, n. 5/6, p. 337, 2002. Disponível em: <http://www.emeraldinsight.com/0957-6053.htm> Acesso em: 14 maio 2004.

BASTOS, A. **Gerenciando a segurança das informações nas empresas.** 1998. Disponível em: <http://www.modulo.com.br/empresa/...as/artigo_entrevista/a-gerenc.htm> Acesso em: 05 abr. 2004.

CARUSO, C. A. A.; STEFFEN, F.D. **Segurança em Informática e de Informação.** 2.ed. São Paulo: SENAC SP, 1999. p. 15, 29, 31.

CERVO, R. **Metodologia científica:** para uso dos estudantes universitários. 3. ed. São Paulo: Mcgraw-Hill do Brasil, 1983. p. 160.

COLTRO, R. Segurança: prioridade corporativa. **Computerworld.** 2002. Disponível em: <http://computerworld.uol.com.br/AdPortalV3/adCmsDocumentoShow.aspx?Documento=18295> Acesso em: 05 abr. 2004.

CRISTONI, I. A segurança, sempre em segundo plano. **Revista Informática Hoje.** São Paulo, Citrix, n. 10, p. 8-9, set. 2000.

DAVENPORT, T. H. **Ecologia da informação:** por que só a tecnologia não basta para o sucesso na era da informação. São Paulo: Futura, 1998.

D`ANDRÉA, E. Ano novo de muito trabalho. **Web Segurança.** Disponível em: <www.itweb.com.br/hotsites/ seguranca/artigo.aspx?id=45662> Acesso em: 20 ago. 2004.

DeMARCO, T.; LISTER, T. **Peopleware:** como gerenciar equipes e projetos tornando-os mais produtivos. São Paulo: Mcgraw-Hill do Brasil, 1990. p. 27 e 31.

DIAS, C. **Segurança e Auditoria da Tecnologia da Informação**. Rio de Janeiro: Axcel Books do Brasil, 2000. p. 4, 54, 56-57, 114.

DRUCKER, P. **Administrando para o futuro.** São Paulo: Pioneira, 1995. p. 22 e 25.

FERREIRA, A.B.H. **Novo dicionário da língua portuguesa**. 2. ed. São Paulo: Nova Fronteira, 1995. p. 170.

FIGUEIRÊDO, L. S. **Segurança da Tecnologia da Informação.** 2002. Disponível em: <http://www.modulo.com.br> Acesso em: 20 maio 2004.

FONTES, E. **Segurança da Informação:** Investimento ou Custo Operacional? Disponível em: <http://www.securenet.com.br/artigo.php?artigo=108> Acesso em: 20 ago. 2004.

GIL, A. C. **Como elaborar projetos de pesquisa.** São Paulo: Atlas, 1988. p. 96.

GONÇALVES, L. R. de O. **O surgimento da Norma Nacional de Segurança de Informação [NBR ISO/IEC-17799:2001].** Disponível em: <http://www.batori.com.br/pag_con.asp?id_pagina=436> Acesso em: 06 jun. 2004.

GUROVITZ, H. Falta de medida. **Revista Exame**. São Paulo: Abril, v. 31, n. 23, p. 40, abr. 2001.

LASALA. K. P. **Human Performance Reliability:** A Historical Perspective. IEEE Transactions on Reliability, v. 47, 1998, p. 5. Disponível em: <http://ieeexplore.ieee.org/xpl/abs_free.jsp?arNumber=740553> Acesso em: 05 abr. 2004.

LAUREANO, M. A. P. **A questão humana na segurança da informação**. 2004. Disponível em: <http://www.ppgia.pucpr.br/~laureano/puc_2004/gst/questão_humana.html> Acesso em: 15 set. 2004.

LEVESON, N. G. et al. Analyzing Software Specifications for Mode Confusion Potential. **Workshop on Human Error and System Development**, 1997. Disponível em: <http://citeseer.ist.psu.edu/context/997826/0> Acesso em: 14 set. 2004.

LOSS CONTROL Consultoria e Assessoria Ltda. – Autotreinamento em Segurança da Informação em CD-ROM da LOSS CONTROL . 2001.

MACEDO, P. de O. **Plano de Contingências do Setor de Tecnologia da Informação para Empresas de Telecomunicações**. Canoas, 2003. 70 f. Trabalho de Graduação (Bacharelado em Ciência da Computação) – Setor de Ciências Exatas, Universidade Luterana do Brasil. p. 19, 22-23, 26.

MARTIN, J. **Engenharia da Informação:** introdução. Rio de Janeiro: Editora Campus, 1991. p. 12.

MOREIRA, S. N. **Segurança mínima:** uma visão coorporativa da segurança de informações. Rio de Janeiro: Axcel Books do Brasil, 2001. p. 11-12 e 27.

REZENDE, D. A.; ABREU, A. F. **Tecnologia da Informação Aplicada a Sistemas de Informação.** São Paulo: Atlas, 2000. p. 18 e 20.

ROCHA, L. F. **Certificação 17799:** uma visão internacional. 2003. Disponível em: <http://www.modulo.com.br/index.jsp> Acesso em: 10 jun. 2004.

SEBRAE. Estatísticas das empresas exportadoras e importadoras. **Classificação por tamanho das empresas.** Disponível em: <http://www.sebrae.com.br/aprendasebrae/exportacao.asp> Acesso em: 29 set. 2004.

SÊMOLA, M. **Perspectivas 2003 para o mercado de segurança da informação.** 2003. Disponível em: <http://www.modulo.com.br/index.jsp> Acesso em: 10 jun. 2004.

SCUDERE, L. **2003: Tendências e previsões para a área de segurança.** 2003. Disponível em: <http://www.timaster.com.br/revista/artigos/main_artigo.asp?codigo=738> Acesso em: 27 jun. 2004.

TSUNODA, D. F. **Segurança de Informações.** Material apresentado na disciplina de Monitoramento da Informação do Curso de Gestão da Informação da UFPR, Curitiba, 2003. p. 4-5.

ZORRINHO, C. **Gestão da informação.** Lisboa: Editora Presença, 1995. p. 32.

ANEXO 1 – CITAÇÃO DO HISTÓRICO DA NBR ISO/IEC 17799

CITAÇÃO DO BREVE HISTÓRICO DA NORMA NBR IEC/ISO 17799 (CÓDIGO DE PRÁTICA PARA A GESTÃO DA SEGURANÇA DA INFORMAÇÃO).

A ISO 17799 se origina de um esforço do governo britânico, que em 1987, através do UK DTI (*Departamente of Trade Center*) criou o CCSC (Comercial *Computer Security Centre*), cujo objetivo era a criação de critérios para a avaliação da segurança e de um código de segurança para os usuários das informações, de uma forma geral. No ano de 1989 foi publicada a primeira versão do código de segurança, que na época foi denominado de PD0003 - Código de Gerenciamento de Segurança da Informação.

Em 1995 esse código foi revisado, ampliado e publicado como uma norma britânica (BS), a BS7799-1:1995 (*Information technology - Code of pratic for information security management*) Em 1996, essa norma foi proposta a I.S.O. para homologação, mas foi rejeitada. Neste mesmo período uma segunda parte deste documento estava sendo criada e foi disponibilizada em novembro de 1997 para consulta e avaliação do público. Em 1998 este documento foi publicado como BS7799-2:1998 *(Information Security Management Systems*).

Em Abril de 1999 as duas normas (a de 1995 e a de 1998) foram publicadas após uma revisão, com o nome de BS7799-1999; neste período esta norma já estava sendo adotada por outros países, como a Austrália, a África do Sul, a República Checa, a Dinamarca, a Coréia, a Suíça e a Nova Zelândia. BS7799 já foi traduzida para várias línguas entre as quais pode-se destacar o Francês, o Alemão e o Japonês.

Neste mesmo ano a primeira parte deste documento foi submetida à "ISO" para homologação, sobre o mecanismo de "*Fast Track*". Em maio de 2000 a "BSI" homologou a primeira parte da norma BS7799. Em outubro na reunião do comitê da "ISO" em Tóquio, a norma foi votada e aprovada pela maioria dos representantes.

Os representantes dos países ricos, excluindo a Inglaterra, foram todos contra a homologação; mas em primeiro de dezembro de 2000 houve a homologação desta "BS" como "ISO/IEC 17799:2000".

A norma BS7799-2 foi submetida a um processo de revisão em 2001, em janeiro de 2002 foi emitido o primeiro *draft* da mesma para acesso e avaliação publica, esta revisão visa ajustar BS7799-2 com normas internacionais, tais como a ISO9001 e a ISO14001, e remover aspectos próprios da lei britânica. Os controles da ISO/IEC 17799 foram adicionados a um anexo desta versão, permitindo uma correspondência entre a numeração em ambas as normas. A BS 7799-2:2002 foi publicada no dia 5 de setembro de 2002 (GONÇALVES, 2004).

ANEXO 2 – MODELO DE FICHA DO CATÁLOGO INDUSTRIAL DO PARANÁ/2004


FIEP
CIEP
SESI
SENAI
IEL
Sistema Federação das Indústrias do Estado do Paraná
Cadastro das Indústrias - Fornecedores e Serviços 2004
Consultas
Mensagem do Presidente
Empresas com Sistema de Qualidade ISO 9001/14001
Cadastro Industrial 2003 Introdução
CNI - Diretoria
Federações das Indústrias do Brasil
Sistema FIEP
Diretoria FIEP
Diretoria CIEP
Conselho Deliberativo
Conselhos Temáticos
Coordenadorias FIEP
Relações dos Sindicatos Patronais filiados a FIEP
SESI - Serviço Social da Indústria
SENAI - Serviço Nacional de Aprendizagem Industrial
IEL - Instituto Euvaldo Lodi
CIN - Centro Internacional de Negócios
Início • Sair
Indústrias
Setor de Atividade
Razão Social
CNPJ
Importadores
Exportadores
Todos
Nº de Empregados
Maior que
Menor que
Entre
e
Nome Fantasia
Município
Produto
Localizar
Limpar
Fornecedores e Serviços
Razão Social
Localizar
Título
Localizar
Resultado da busca
Informações da Empresa
Home Page
E-mail
Veja Anúncio
Imprimir

ANEXO 3 – EMPRESAS DE GRANDE PORTE DO MUNICÍPIO DE CURITIBA (UNIVERSO DA PESQUISA)

ANEXO 4 – QUESTIONÁRIO

Universidade Federal do Paraná
Departamento de Ciências Sociais Aplicadas
Curso de Gestão da Informação
Disciplina: Projeto de Pesquisa em Informação (Trabalho de Conclusão de Curso)
Orientadora: Profª. Dra. Patricia Zeni Marchiori

QUESTIONÁRIO

Nome da Empresa:
Responsável pela Segurança da Informação:

Curitiba, dd de outubro de 2004.

Prezado(a) Senhor(a):

Conforme contato telefônico prévio (em dd/mm/2004), o presente instrumento de coleta tem como finalidade investigar:

a) como as empresas estão tratando a questão da segurança da informação;
b) verificação dos mecanismos técnicos e não técnicos valorizados pelas empresas quanto à questão da segurança da informação;
c) o grau de utilização da NBR ISO/IEC 17799.

Por favor, responda todas as questões escolhendo a alternativa que melhor corresponda ao seu ambiente organizacional. Esclareço que as **respostas serão tratadas de maneira confidencial e que as informações levantadas serão utilizadas exclusivamente para o desenvolvimento do proposto trabalho, nenhuma empresa ou pessoa será identificada em particular.** Peço ainda, que o questionário devidamente preenchido seja devolvido, via e-mail ou conforme tenha sido combinado anteriormente, até o dia 22 de outubro de 2004.

Caso tenha dúvidas no esclarecimento deste, favor entrar em contato com Isabela Drago, através do telefone: 9927-5202 ou via e-mail: isabela_drago@yahoo.com.br ou com a orientadora da presente pesquisa Profª. Dra. Patricia Zeni Machiori, telefone: 9977-9804, e-mail: pzeni@ufpr.br.

Agradeço antecipadamente a sua indispensável colaboração.

- Envio do Questionário:

  Opção Correio: Rua Belém, 20 – apto. 51 – Cabral
  CEP 80035-170 – Curitiba/PR.

  Opção E-mail: isabela_drago@yahoo.com.br

Isabela Drago

Isabela Drago

---

1. Qual das definições abaixo se enquadra ao que a sua empresa entende por “Segurança da Informação”?

   ❑ “É a preservação da confidencialidade, integridade e disponibilidade da informação”.[1]

   ❑ “É um conjunto de medidas que se constituem basicamente de controles e política de segurança, tendo como objetivo a proteção das informações dos clientes e da empresa, controlando o risco de revelação ou alteração por pessoas não autorizadas”.[2]

   ❑ “Todas as informações têm a interferência de um ser humano no processo ou tecnologia, neste caso é necessário garantir a confiabilidade humana nas partes envolvidas”.[3]

   ❑ A empresa define como “Segurança da Informação” o que segue (favor descrever):

   _____

   ❑ Nenhuma das definições.

[1] Código de prática para a gestão da segurança da informação. **NBR ISO/IEC 17799**, 2001, p. 04.

[2] BRADESCO. **Segurança da Informação**. Disponível em: <http://www.bradesco.com.br> Acesso em: 10 ago. 2004.

[3] LASALA, K. P. Human Performance Realiability: A Historical Perspective. IEEE Transactions on Reliability, vol. 47, 1998.

2. Considerando, hipoteticamente, que você **concorde** com a seguinte frase: “a segurança da informação é fonte de vantagem competitiva”, as razões de sua **concordância** seriam:

   * Indique conforme a escala crescente de importância (1 = mais importante e 4 = menos importante).

	Garantia da confidencialidade da informação;
	Garantia da integridade da informação;
	Garantia da disponibilidade da informação;
	Outros: _____

3. Considerando, hipoteticamente, que você **discorde** com a seguinte frase: “a segurança da informação é fonte de vantagem competitiva”, as razões de sua **discordância** seriam:

   * Indique conforme a escala crescente de importância (1 = mais importante e 4 = menos importante).

	Existência de altos custos envolvidos;
	Dificuldades de envolvimento dos funcionários;
	Desconhecimento do assunto no ambiente da empresa;
	Outros: _____

4. Quanto às questões sobre segurança da informação listadas abaixo. Indique, aquelas que foram alvo de discussão em sua empresa (assinale quantas desejar):

   - ❑ O que proteger?
   - ❑ Contra que ou quem?
   - ❑ Quais as ameaças mais prováveis?
   - ❑ Qual a importância de cada recurso de informação?
   - ❑ Qual o grau de proteção desejado?
   - ❑ Quanto tempo, recursos humanos e financeiros se pretende gastar para atingir os objetivos de segurança desejados?
   - ❑ Quais as expectativas dos usuários e clientes em relação à segurança da informação?
   - ❑ Quais as conseqüências para a instituição se seus sistemas e informações forem violados ou roubados?
   - ❑ Outros. Quais? _____
   - ❑ Prefiro não opinar.

5. Quanto aos objetivos relativos à segurança da informação listados abaixo. Indique no máximo três deles que seriam valorizados por sua empresa.

   - ❑ **Confidencialidade/privacidade:**
     Proteger as informações contra acesso de qualquer pessoa não autorizada.
   - ❑ **Integridade de dados:**
     Evitar que dados sejam apagados, ou alterados sem a permissão.
   - ❑ **Legalidade:**
     Estado legal da informação, em conformidade com os preceitos da legislação em vigor.
   - ❑ **Disponibilidade:**
     Garantir o provimento do serviço de informática, sob demanda e sempre que necessário, aos usuários autorizados.
   - ❑ **Consistência:**
     Certificar-se de que o sistema atua de acordo com a expectativa dos usuários.
   - ❑ **Isolamento ou uso ilegítimo:**
     Controlar o acesso ao sistema. Garantir que somente usuários autorizados tenham acesso ao sistema.
   - ❑ **Auditoria:**
     Proteger os sistemas contra erros e atos cometidos por usuários autorizados.
   - ❑ **Confiabilidade:**
     Garantir que, mesmo em condições adversas, o sistema atuará conforme esperado.

- ❑ Outros. Quais? _____
- ❑ Prefiro não opinar.

6. Assinale os **mecanismos técnicos** utilizados em sua empresa para a garantia da segurança da informação.
   - ❑ Senhas fortes que proíbam o acesso não autorizado aos sistemas.
   - ❑ Manuseio técnico adequado de informações confidenciais/críticas.
   - ❑ Investimento em tecnologias de informação.
   - ❑ Outros. Quais?_____
   - ❑ A empresa não utiliza de quaisquer mecanismos.
   - ❑ Prefiro não opinar.

7. Em relação aos aspectos **não tecnológicos** envolvidos com a segurança da informação, indique aquele que sua empresa considera mais importante (marque apenas um).
   - ❑ Existência de uma política de segurança da informação.
   - ❑ Comprometimento contínuo dos funcionários.
   - ❑ Esclarecimento dos funcionários.
   - ❑ Outros. Quais?_____
   - ❑ Prefiro não opinar.

8. Com relação aos procedimentos de segurança da informação da empresa o **custo** é um fator relevante?
   ( ) Não ( ) Sim. Quais? (assinale quantas desejar)
   - ❑ Custo dos equipamentos;
   - ❑ Custo dos softwares;
   - ❑ Custo relativo à treinamento;
   - ❑ Custo de contratação de especialistas/consultores;
   - ❑ Custo decorrente da implantação/manutenção do "Código de Prática para a Gestão da Segurança da Informação - NBR ISO/IEC 17799" (se for o caso);
   - ❑ Outros. Quais? _____
   - ❑ Prefiro não opinar.

9. Sua empresa aplica o **Código de Prática para a Gestão da Segurança da Informação** (NBR ISO/IEC 17799)?
   ( ) Sim ( ) Não

10. Caso sua empresa aplique a norma NBR ISO/IEC 17799, indique o que já foi/está sendo incrementado:
    - ❑ **Política de Segurança**:
      Prover orientação e apoio à empresa para a segurança da informação.
    - ❑ **Segurança organizacional**:
      Prover infra-estrutura de segurança da informação na organização;
    - ❑ **Classificação e controle dos ativos de informação**:
      Manter a proteção adequada dos ativos de informação;
    - ❑ **Segurança em pessoas**:
      Reduzir os riscos de erro humano, roubo, fraude ou uso indevido de instalações;
    - ❑ **Segurança física e do ambiente**:
      Prevenir acesso não autorizado, dano e interferência às informações e instalações físicas da organização;

- ❑ **Gerenciamento das operações e comunicações**:
  Garantir a operação segura e correta dois recursos de processamento da informação;
- ❑ **Controle de acesso**:
  Controlar o acesso à informação;
- ❑ **Desenvolvimento e manutenção de sistemas**:
  Garantir que a segurança seja parte integrante dos sistemas de informação;
- ❑ **Gestão da continuidade do negócio**:
  Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos;
- ❑ **Conformidade**:
  Garantir conformidade dos sistemas com as leis, estatutos, regulamentações, obrigações contratuais, políticas e normas organizacionais de segurança e de quaisquer requisitos de segurança.

- Indique sua área de formação (OPCIONAL):

❑ Administração
❑ Automação Industrial
❑ Economia
❑ Informática
❑ Engenharia
❑ Gestão da Informação
❑ Outra. Indique: _____